AVAST! antivirus Edition Familiale Version 4.8

Guide d'utilisateur

SOMMAIRE

Introduction

Bienvenue sur avast! antivirus Edition Professionnelle version 4.8.

avast! 4 antivirus est une collection des technologies de pointe, décorées par des prix prestigieux, qui travaillent dans une parfaite synergie pour un but commun : protéger votre système et vos données contre les virus informatiques. Dans sa gamme, il représente le meilleur choix pour n'importe quel poste de travail équipé d´un système Windows.

avast! antivirus incorpore une technologie d’anti-spyware, certifiée par West Coast Lab’s Checkmark process, aussi bien qu’un anti-rootkit et de fortes capacités d’auto-protection pour assurer continuellement la protection de vos programmes et données de valeur.

A propos d’ALWIL Software a.s.

Depuis 1988, ALWIL Software a produit des logiciels d’antivirus qui ont été développés dans la gamme de produits multi-primés avast! antivirus, rendant avast! l'un des produits les plus matures et éprouvés sur le marché d’antivirus.

Ayant son siège social à Prague, en République tchèque, ALWIL Software développe et vend les produits avast! antivirus qui protègent tous les principaux systèmes d'exploitation et tous les grands types de dispositif vulnérables. Pour plus de détails sur l'entreprise et ses produits, veuillez-vous référer à notre site Web: www.avast.com

avast! ® est une marque déposée aux États-Unis d'Amérique et dans d'autres pays et est utilisée sous licence exclusive d'ALWIL Software a.s.

Aide supplémentaire

Si vous rencontrez des difficultés avec votre programme avast! antivirus et que vous n’êtes pas en mesure de les résoudre après avoir lu ce manuel, vous pouvez trouver la réponse dans le Centre de Support de notre Site web à http://support.avast.com

- Dans la section de la Base de connaissances, vous pouvez rapidement trouver la réponse à certaines des questions les plus fréquemment posées

- Alternativement, vous pouvez profiter du forum de support d’avast ! là, vous pouvez interagir avec d'autres utilisateurs d'avast ! qui ont peut être connu le même problème et ont déjà découvert la solution. Vous devez vous inscrire pour utiliser le forum mais cela est très rapide et simple. Pour vous inscrire afin d’utiliser le forum, référez-vous à http://forum.avast.com/

Si vous ne parvenez toujours pas à résoudre votre requête, vous pouvez "Soumettre un incident" à notre équipe de support. Encore une fois, vous devez vous inscrire pour le faire et lorsque vous nous écrivez, s'il vous plaît assurez-vous d'inclure le maximum d'informations possible.

Menaces sur votre ordinateur

Les virus, logiciels espions, rootkits et toutes les formes de logiciels malveillants sont collectivement connus sous le nom de logiciels malveillants ; Un logiciel malveillant est aussi souvent appele "badware".

Qu'est-ce que c'est qu'un virus?

Un virus informatique est un bout de logiciel habituellement malveillant dans sa nature, qui est utilisé pour se propager lui-même ou propager d'autres logiciels du même genre d'un ordinateur à un autre. Les virus eux-mêmes peuvent causer des dommages du système, perte de données de valeur, ou peuvent-être utilisés pour installer des logiciels espions (spyware), des rootkits ou d'autres logiciels malveillants sur un système vulnérables.

Un moyen clé de prévenir l'infection est d'avoir une solution d'antivirus à jour installée sur tous les ordinateurs d'un réseau, et de faire en sorte que tous les derniers correctifs de sécurité du système d'exploitation soient installés. Les utilisateurs doivent également faire attention et s'assurer que les sources des logiciels qu'ils téléchargent à partir de l'internet sont saines car plusieurs types de logiciels malveillants sont installés durant la recherche d'autres logiciels légitimes.

Qu'est-ce que c'est qu'un logiciel espion (spyware)?

Un logiciel espion (Spyware) est un logiciel conçu pour collecter des informations sur l'utilisateur de l'ordinateur sur lequel il est installé et cela souvent sans son consentement ou sans qu'il ne le sache. Cette information peut-être le résultat de ce qu'on appelle le vol d'identité, ou vol d'informations précieuses (telles que des informations relatives à une banque ou à une carte de crédit).

De nos jours, la plupart des logiciels espions est actuellement mis au point par des réseaux de crime organisé, plutôt que des individus isolés opportunistes et est installée par un virus ou une autre forme de logiciel malveillant (malware).

Qu'est-ce que c'est que les rootkits?

Les rootkits sont des programmes qui s'installent sur votre système, tout en se cachant eux-mêmes, leurs processus, leurs services et leurs clés de registre, afin de rester invisible à l'utilisateur. Ils représentent un risque pour la sécurité des réseaux informatiques domestiques et d'entreprises et sont notoirement difficiles à trouver et à supprimer.

Les rootkits eux-mêmes sont normalement déployés par un autre infection de logiciel malveillant (exemple : un cheval de Troie), et il est donc fortement recommandé que les utilisateurs d'ordinateur aient un système d'antivirus / anti-spyware (anti-espion) mis à jour, installé et opérationnel sur leur PC. Un tel système est bel et bien d'avast! antivirus 4.8.

Caractéristiques principales d'avast ! antivirus

avast! est un produit multi-primé dans la gamme des produits d'antivirus développé par ALWIL Software, il est certifié par les laboratoires ICSA et Checkmark (en qualité d'antivus et anti-malware). avast! antivirus reçoit régulièrement le prix de Virus Bulletin 100% pour la détection de 100% des virus "in the Wild" et il est récidive lauréate de Secure Computing Award.
Avast! antivirus est utilisé dans environ 75 millions de maisons et bureaux partout dans le monde entier, il est spécifiquement conçu pour exiger peu de ressource du système et effectue de façon progressive et automatique les mises à jour du programme ainsi que celles de la base de données virale, ce qui lui donne d'être toujours à jour.
avast! 4 Edition Professionnelle est une collection des technologies de pointe concue pour vous apporter une protection incomparable contre tous les formes de logiciels malveillants. Les caractéristiques principales d'avast antivirus Edition familiale et Edition Professionnelle sont comparées et décrites ci-dessous.

Caractéristiques principales	**Edition Familiale**	**Edition Professionnelle**
Noyau d'Antivirus basé sur un moteur antivirus de haute performance	**Oui**	**Oui**
protection résidente solide	**Oui**	**Oui**
anti-spyware (anti-espion) incorporé	**Oui**	**Oui**
détection de rootkit incorporée	**Oui**	**Oui**
Autoprotection solide	**Oui**	**Oui**
Mises à jour automatiques et incrémantales	**Oui**	**Oui**
Zone de quarantaine pour conserver les fichiers suspects	**Oui**	**Oui**
Intégration au système	**Oui**	**Oui**
Nettoyeur de virus intégré	**Oui**	**Oui**
Scanner en ligne de commande	**Non**	**Oui**
Bloquer de script	**Non**	**Oui**
Mises à jour PUSH	**Non**	**Oui**
Interface utilisateur avancée, capacité de créer et de planifier des tâches définies.	**Non**	**Oui**

Noyau antivirus

Le noyau antivirus est le cœur du programme. La dernière version du Noyau antivirus avast! possède des capacités de détection élevées, ainsi qu'une performance remarquable. Vous pouvez vous attendre à 100% de détection des virus menaçants actuellement le monde informatique, et une détection excellente des chevaux de Troie.
Le noyau est certifié par les laboratoires ICSA; il participe fréquemment aux essais du magazine Virus Bulletin, remportant souvent le prix VB100.

Protection résidente (ou protection "à l'accès")

De nos jours, la Protection Résidente (la protection en temps réel du système de l'ordinateur), est l'une des plus importantes caractéristiques d'un programme d'antivirus. La protection résidente d'avast! est une combinaison de plusieurs parties ou " modules résidents" qui sont capables de détecter un virus avant même qu'il n'ait une occasion quelconque d'infecter votre ordinateur.

Technologie d'anti-spyware (anti-espion) incorporée

avast! antivirus possède maintenant un module complet incorporé de détection et de suppression des logiciels espions qui est certifié par les Laboratoires West Coast Lab's Checkmark et qui offre une protection encore plus complète de vos programmes et données de valeur.

Technologie d'anti-rootkit incorporée

Une technologie d'anti-rootkit basé sur une technologie de pointe de GMER est aussi incorporee dans le programme.

Si un rootkit est découvert, il est d'abord desactive et ensuite, s'il peut être supprimé sans nuire à la performance de l'ordinateur, il est supprimé. avast! antivirus comprend une base de données des virus qui peuvent être automatiquement mis à jour pour fournir une protection continue contre les rootkits.

Puissante auto-protection

Certains virus peuvent essayer de désactiver le logiciel d'antivirus d'un ordinateur. Afin d'assurer le bon fonctionnement de votre protection, même contre les dernières menaces qui peuvent mettre hors service votre protection de sécurité, un puissant module d'auto-défense a été intégré à avast ! Ceci est basé sur la technologie multi-primée d'avast! antivirus et fournit une couche supplémentaire de sécurité pour assurer que vos données et programmes sont toujours protégés.

Mises à jour Automatiques

Les mises à jour automatiques représentent un autre besoin clé dans la protection contre les virus. Cela concerne aussi bien la base des données virales que le programme lui-même. Les mises à jours sont incrémentales, seules les données nécessaires sont téléchargées, ce qui diminue considérablement la taille des transferts. La taille typique des mises à jour de la base virale est de quelques dizaines de KB; les mises à jour de programme sont typiquement de quelques centaines de KB.
Si votre connexion internet est permanente (comme la connexion à large bande), les mises à jour s'effectuent automatiquement à intervalles réguliers. Si vous vous connectez à l'Internet occasionnellement, avast! observe votre connexion et essaye d'exécuter la mise à jour lorsque vous êtes en ligne. Cette caractéristique est décrite en profondeur à la page 37.

La Zone de quarantaine

La zone de quarantaine peut être vue comme un dossier logé sur votre disque dur et qui a des propriétés spéciales; ce qui lui donne d'être un endroit sûr et isolé pour le stockage des fichiers spécifiques. Vous pouvez toujours travailler avec les fichiers qui sont dans la zone de quarantaine, mais avec quelques restrictions de sécurité.

La propriété principale de la Zone de quarantaine est : l'isolation complète par rapport au reste du système d'exploitation. Aucun processus extérieur, comme un virus, ne peut avoir accès aux fichiers qui y sont et aussi, du fait que les fichiers qui sont à l'intérieur de la Zone de quarantaine ne peuvent pas être exécutés, il n'y a aucun danger de stocker les virus à cet endroit. Pour plus d’informations, voir la page 48.

Intégration au système

Avast ! Antivirus s'intègre parfaitement à votre système. Un scan peut être lancé directement à partir de l'explorateur de Windows, en cliquant-droit (un clic avec le bouton droit de votre souris) sur un dossier ou un fichier et en choisissant la sélection correspondante à partir du menu.
Un économiseur d’écran spécial est aussi fourni, celui-ci lance un scan quand il est en exécution. Avast ! antivirus travaille ensemble avec votre économiseur d’écran préféré, donc vous n’avez pas à changer vos réglages personnels pour l’utiliser. Pour régler l’écran de veille d’avast!, veuillez vous référer à la page 73.

Dans la version 32-bit de Windows NT/2000/XP/Vista, il est aussi possible de lancer un “scan au démarrage du système” qui vous permet d’analyser le système pendant qu’il est en démarrage et avant qu’un virus ne soit activé. Ceci est utilie dans le cas où vous soupconnez la présence d’un virus sur votre ordinateur.

Nettoyeur de virus (Virus Cleaner) intégré

avast! antivirus est essentiellement conçu pour protéger votre ordinateur contre les infections virales ou d'autres formes de malware. Sa fonction première est de prévenir plutôt que guérir. Toutefois, il intègre maintenant un Nettoyeur de Virus (Virus Cleaner) qui est capable de supprimer des ordinateurs infectés, certains des virus les plus rependus. Malheureusement, le nombre de virus en circulation ne cesse de croître et dans le cas où votre ordinateur est infecté par des virus qui ne peuvent pas être supprimés par le Nettoyeur de Virus (Virus Cleaner), il serait nécessaire d'obtenir l'assistance d'un expert.

Plus d'informations sur le Nettoyeur de Virus peuvent être trouvées sur www.avast.com

Scanneur en ligne de commande (Uniquement pour l’Edition professionnelle)

Pour les utilisateurs expérimentés, l'Édition Professionnelle dispose d’un scanneur en ligne de commande. Le programme ashCmd utilise exactement le même noyau d’analyse qu’avast!, ce qui donne exactement le même résultat. Le scan peut être contrôlé par

beaucoup d'arguments et commutateurs; pour l’utiliser comme un ‘‘pipe filter’’; et un mode STDIN/STDOUT spécial est disponible. Le module est prévu pour être utilisé dans des programmes BATCH. Son rendement est identique à celui des tâches de l’Interface Utilisateur Avancée (y compris les fichiers de rapport).

Bloqueur de Script (Uniquement pour l’Edition professionnelle)

Le bloqueur de script intégré est un module qui protège votre ordinateur contre les virus de script cachés à l'intérieur des pages web. Ces scripts sont normalement inoffensifs parce que les programmes qui les animent les empêchent d'accéder à aucuns fichiers. Toutefois, ils peuvent être un trou de sécurité dans un navigateur. Cette faille pourrait être exploitée par un virus qui pourrait infecter votre ordinateur. avast! donc vérifie les pages Web que vous visitez en analysant tous les scripts pour détecter ceux qui pourraient être potentiellement dangereux.

Mises à jour PUSH (Uniquement pour l’Edition professionnelle)

Les mises à jour PUSH représentent une fonction spéciale de l'Édition Professionnelle. C'est un changement impressionnant dans la philosophie des mises à jour. Habituellement, chaque programme installé vérifie régulièrement la disponibilité de nouvelles mises à jour. Les Mises à jour PUSH, cependant, sont lancées par notre serveur; elles aboutissent à votre ordinateur répondant rapidement et effectuant l'exécution de la mise à jour nécessaire. Le système est basé sur le protocole SMTP (c'est-à-dire le même utilisé pour les messages de courrier électronique habituel). La mise à jour elle-même est contrôlée par les services d'avast! (MS Outlook et Courrier Électronique). Le système de PUSH est protégé par un cryptage asymétrique empêchant l'utilisation frauduleuse du protocole.

Interface Utilisateur Avancée (Uniquement pour l’Edition professionnelle)

avast! Antivirus Edition Professionnelle inclut une interface Utilisateur Avancée a partir de laquelle il est possible de créer des “tâches” qui peut être planifiée pour s'exécuter à un moment précis dans l'avenir ou de manière periodique, par exemple quotidiennement, hebdomadairement ou mensuellement. A chaque fois qu'une tâche est exécutée, une nouvelle "session" est créée et c’est dans celle-ci que les résultats de scan sont stockées et peuvent ensuite être visualisées. À la différence de l’Interface Utilisateur Simplifiée, lorsque vous travaillez avec l’Interface Utilisateur avancée, il est possible de spécifier d’avance les actions à exécuter si un virus est détecté. Par exemple, vous pouvez faire les réglages pour que le programme tente immédiatement de réparer les fichiers infectés. Il est également possible de spécifier une action de remplacement si la première action échoue. Par exemple, si un fichier ne peut pas être réparé, il peut être automatiquement déplacé vers la zone de quarantaine.

Système Requis

Les configurations du matériel décrites ci-dessous, représentent les spécifications **minimum** du système recommandé pour le système d'exploitation.

Pour un ordinateur exécutant Windows® 95/98/Me:
486 Processor, 32MB RAM et 100 MB d'espace libre de disque dur.

Pour un ordinateur exécutant Windows® NT® 4.0:
486 Processor, 24MB RAM et 100 MB d'espace libre de disque dur et le Service Pack 3 (ou supérieur) installé

Pour un ordinateur exécutant Windows® 2000/XP® (non pas le Serveur):
Pentium class Processor, 64MB RAM (128MB recommendés) et 100 MB d'espace libre de disque dur

Pour un ordinateur exécutant Windows® XP® 64-bit Edition:
Un AMD Athlon64, Opteron ou Intel EM64T-enabled Pentium 4 / Xeon processor, 128MB RAM (256MB recommendés) et 100 MB d'espace libre de disque dur

Pour un ordinateur exécutant Windows® Vista:
Pentium 4 processor, 512MB RAM et 100 MB d'espace libre de disque dur.
Le programme lui même requiert environ 60MB d'espace libre de disque dur; le reste de l'espace recommandé est réservé à la Base de Données de Rétablissement Viral et son index (VRDB, aussi connue sous le nom de la "Base de données d'intégrité" dans la version précédente).

Un **MS Internet Explorer 4 fonctionnel** ou supérieur est requis pour que le programme fonctionne.

Ce produit **ne peut être intallé sur un système d'exploitation serveur** (Serveurs du même groupe que Windows NT/2000/2003).

Note : De divers problèmes peuvent survenir à la suite de l'installation de plus d'un produit de sécurité sur le même ordinateur. Si vous avez déjà installé un autre logiciel de sécurité, il est recommandé que celui-ci soit désinstallé avant d'essayer d'installer avast!

Comment installer avast! antivirus Edition Familiale

Cette section décrit comment télécharger et installer avast! antivirus Edition Familiale sur votre ordinateur, comment insérer votre clé de licence dans le logiciel une fois le téléchargement et l'installation sont effectués. Les captures d’écrans montrées sur les pages suivantes sont telles qu'elles apparaissent dans Windows XP et peuvent être légèrement diffèrentes dans d'autres versions de Windows.

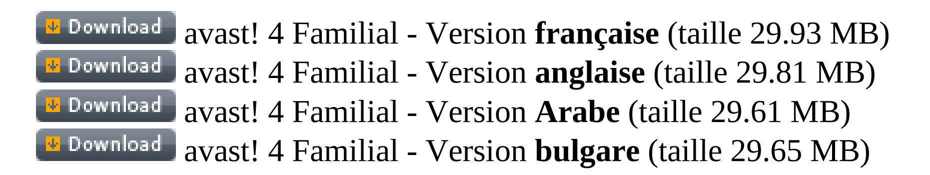
avast! antivirus Edition Familiale peut être téléchargée à partir de www.avast.com.

Il est fortement recommandé que tous les autres programmes soient fermés avant de commencer le téléchargement.

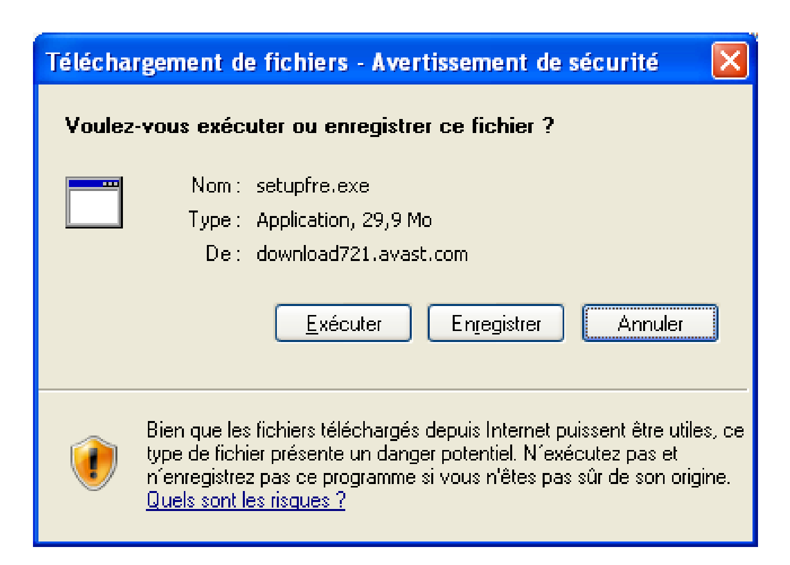
Cliquez sur “Télécharger” puis “Télécharger les programmes” et ensuite sélectionnez la version à télécharger.

A partir de liste des langues disponibles, sélectionnez la version de langue souhaitée – voir ci-dessous – et cliquez sur le bouton “Download”.

Téléchargement d'avast! 4 Edition Familiale



Si vous utilisez Internet Explorer comme navigateur Web, la boîte ci-dessous sera ensuite présentée:



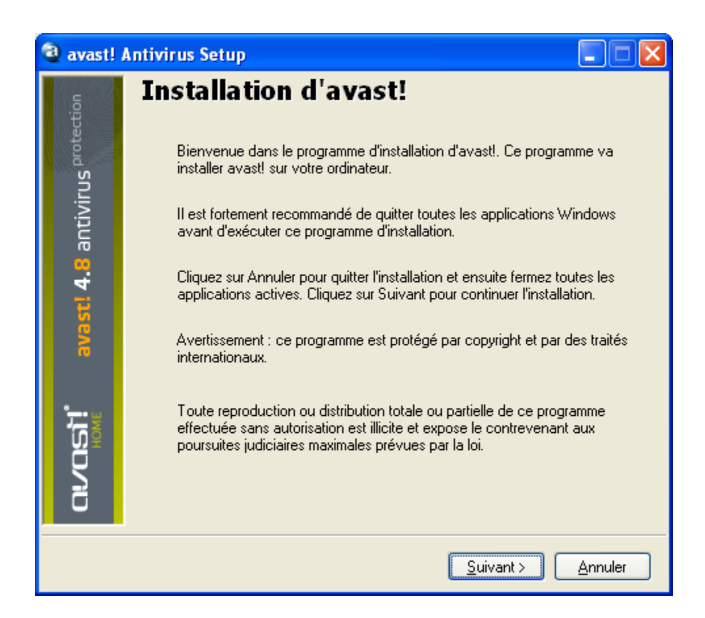
Cliquez sur "Exécuter" ou "Enregistrer" pour commencer le téléchargement du fichier d'installation "Setupfre.exe" sur votre ordinateur.

Si vous voulez qu'avast s'installe immédiatement sur votre ordinateur après que le téléchargement du fichier d'installation soit terminé, cliquez sur " Exécuter ". Une fois que le fichier d'installation est téléchargé complètement, la fenêtre suivante s'affichera :



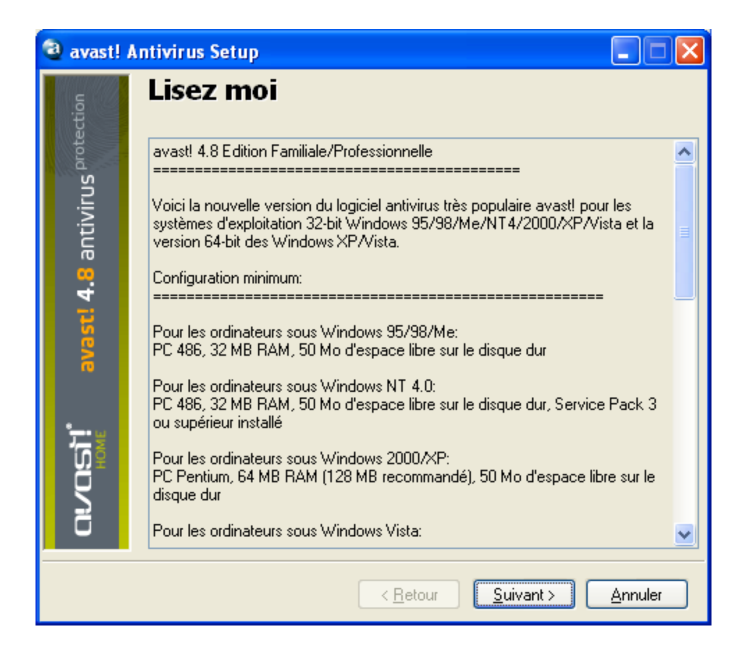
Dans d'autres navigateurs Web, vous pouvez seulement avoir l'option pour "Enregistrer" le fichier. En cliquant sur "Enregistrer" le logiciel sera téléchargé sur votre ordinateur mais il ne sera pas installé à ce moment-là. Pour compléter le processus d'installation, il sera nécessaire de lancer le fichier d'installation "Setupfre.exe" donc souvenez vous de l'endroit où il a été enregistré! Double-cliquez sur le fichier pour l'exécuter.

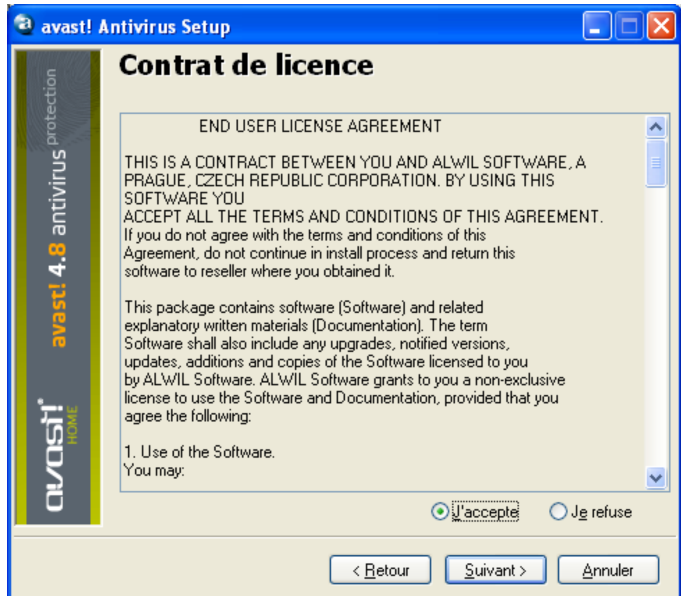
En cliquant encore sur "Exécuter" vous obtiendrez l'écran d'installation d'avast!:



Cliquez sur "suivant" et l'instance d'installation vous guidera pendant le rest du processus d'installation.

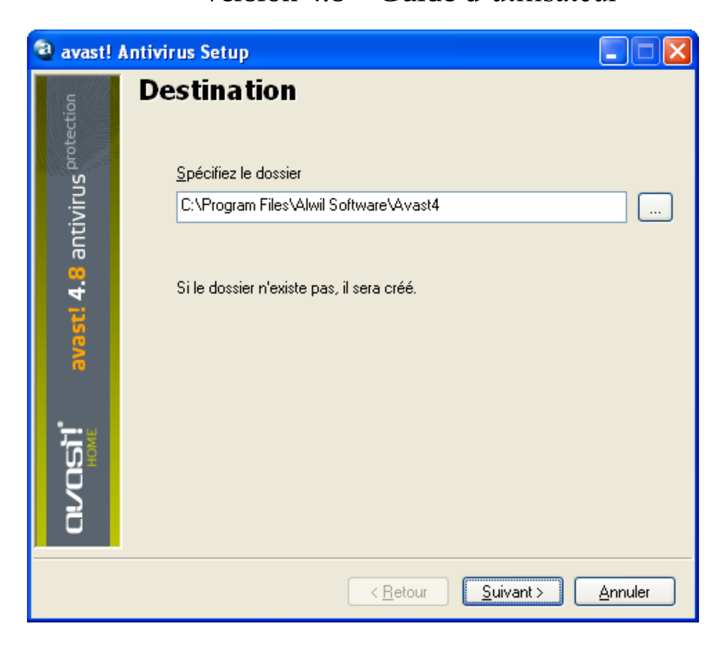
Tout d'abord il vous sera demandé de lire les informations concernant la configuration minimale de système requis, puis de confirmer si vous êtes d'accord avec les conditions de license de l'utilisateur final - voir les deux écrans ci-dessous.



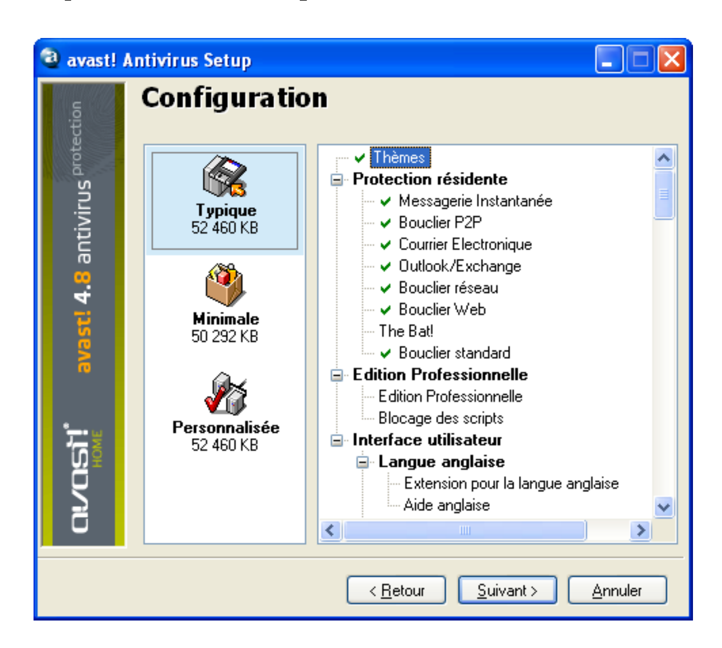


Pour continuer, il est nécessaire de cocher "J'accepte" puis "Suivant".

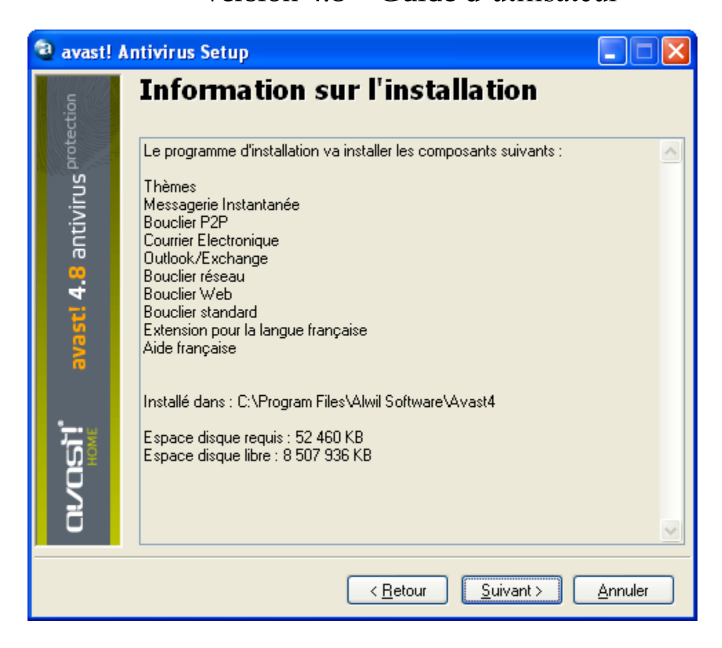
Vous serez alors invité à confirmer le répertoire de destination, c'est-à-dire où les fichiers du logiciel doivent être sauvegardés. Le programme la sélectionnera automatiquement ou créera un nouveau répertoire, si celui-ci n'existe pas déjà. Il est recommandé d'accepter le répertoire de destination par défaut et cliquez simplement sur "Suivant" pour continuer.



Sur l'écran suivant, il vous sera demandé de confirmer la configuration. Les options qui conviennent à la plupart des utilisateurs sont automatiquement sélectionnées. Sauf si vous souhaitez changer tout les paramètres par défaut, par exemple, choix de la langue. Si non, il vous suffit de cliquer sur "Suivant" pour continuer.

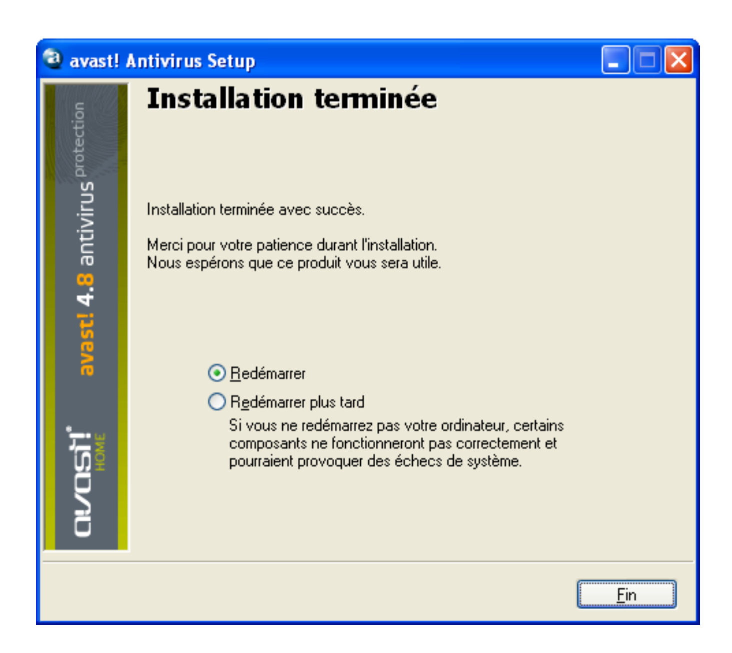


Le programme confirmera ensuite ce qui doit être installé et l'endroit ainsi que la quantité d'espace de disque exigée et disponible. Cliquez "Suivant" pour continuer.



Il vous sera demande ensuite si vous souhaitez planifier une analyse au démarrage du système - voir page 38.

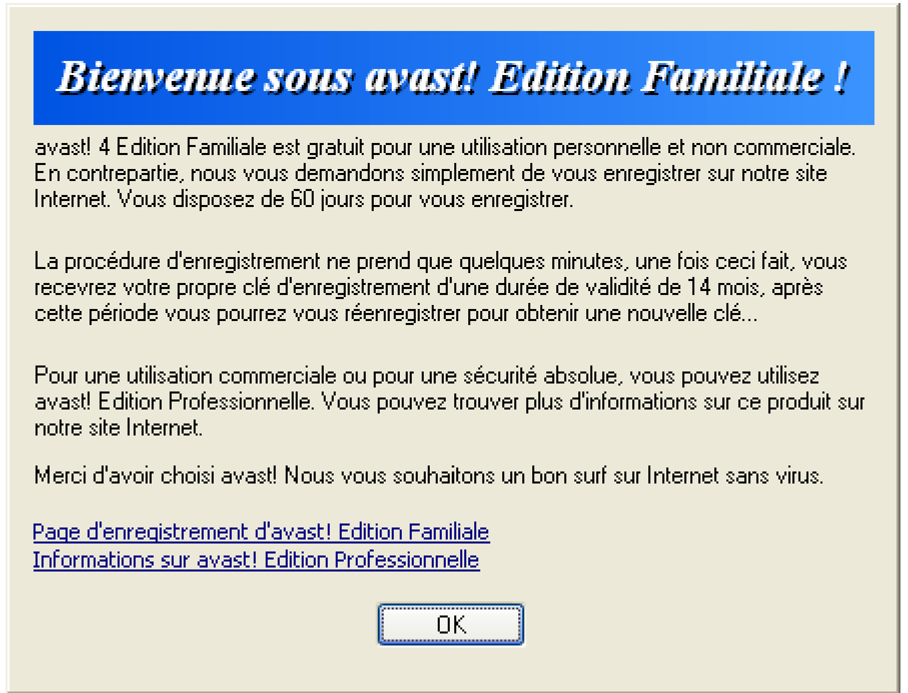
L'écran final devrait confirmer que l'installation a été achevée avec succès. Cependant, pour terminer complètement le processus d'installation, il sera nécessaire de redémarrer votre ordinateur.
Avec "Redémarrer" sélectionné, cliquez sur "Terminer" et votre ordinateur sera automatiquement redémarré.



L'installation est maintenant complète.

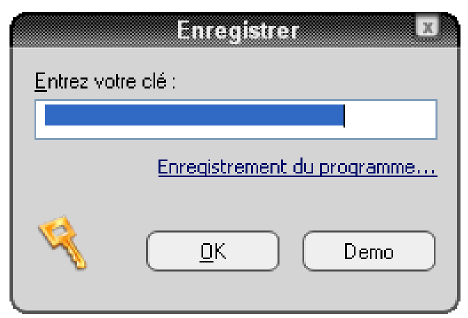
Pour commencer

Après le redémarrage de votre ordinateur, cet écran sera affiché et vous devriez voir une icône sphérique bleue "une sorte de boule" en bas à droite de votre écran, à côté de l'horloge.



Avast antivirus Edition familiale peut être utilisée gratuitement pendant les 60 premiers jours après la première installation, mais à la fin cette période, si vous voulez continuer à l'utiliser, vous devriez vous enregistrer (gratuitement) pour obtenir une clé de licence.

Par conséquent, la première fois que vous exécuterez le programme, vous verrez l'écran suivant:



Il n'est pas nécessaire d'insérer une clé de license de suite. Si vous souhaitez exécuter le programme pour un maximum de 60 jours sans une demande de clé de license, il vous suffit de cliquer sur "Demo". Toutefois, vous pouvez demander une clé de license

maintenant en cliquant sur "Enregistrement du programme" et en suivant la procédure décrite dans la section suivante.

Une fois que vous avez choisi d'exécuter la version de démonstration, cette boîte de dialogue ne s'affiche pas la prochaine fois que vous exécutez le programme. Toutefois, vous pouvez demander une clé de license à tout moment - voir la page suivante "Comment s'inscrire pour obtenir une clé de license"

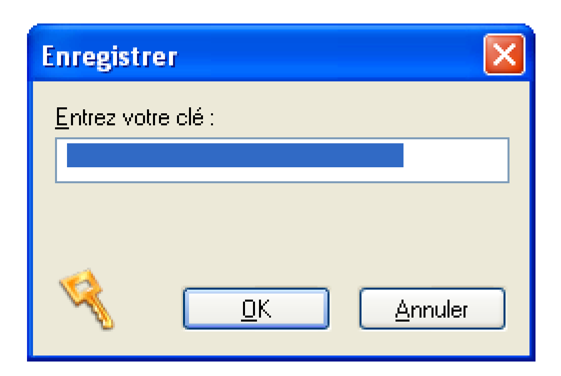
Après 60 jours, si aucune clé de license n'est insérée, l'avertissement suivant s'affiche dans le coin inférieur droit de l'écran de votre ordinateur:



Le message suivant sera affiché à chaque fois que vous demarrerez le programme:



En cliquant sur "OK" vous aurez la fenêtre d'enregistrement ci-dessous qui s'affichera:



La procédure d'obtention et d'insertion de la clé de licence est décrite sur les pages suivantes.

Protection par un mot de passe

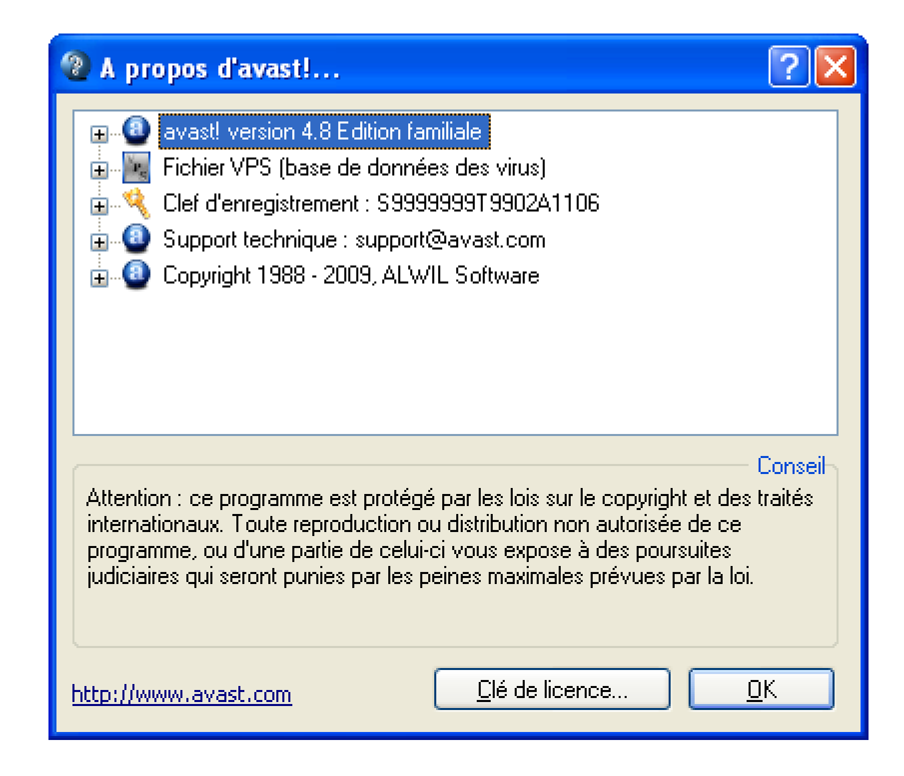
Par un clic droit sur la boule bleua boule bleue-(a) se trouvant dans le coin en bas à droite de l'écran et en sélectionnant "Definir / changer le mot de passe", vous pouvez créer un mot de passe pour protéger votre antivirus contre les modifications non autorisées.

Comment s'enregistrer pour obtenir une clé de licence

Si vous souhaitez continuer à utiliser le programme après 60 jours d'essai gratuit, vous aurez besoin de vous enregistrer pour obtenir une clé de licence valide que vous devriez insérer dans le programme.

Pour obtenir une clé de licence, aller à www.avast.com et pointez le curseur de la souris sur "Support" en haut de la page. Puis cliquez sur "Enregistrement GRATUIT d'avast! Familial". Alternativement, si vous avez déjà téléchargé et installé le programme, cliquez avec le bouton droit de votre souris sur l'icône d'avast! (boule bleue-(a)) qui se trouve dans la barre des tâches à côté de l'horloge et sélectionnez " A propos d'avast !..." dans le menu.

Dans la boîte de dialogue qui apparaîtra, cliquez sur le bouton "clé de licence".



La boîte d'enregistrement apparaîtra – cliquez sur ''Enregistrement du programme''.

Vous serez redirigé sur le site web d’avast! où vous pouvez sélectionner l’option qui vous convient puis remplir le formulaire d’enregistrement. Ensuite cliquez sur le bouton ‘‘Enregistrer’’. Une clé de licence vous sera envoyée à votre adresse e-mail dans les 24 heures qui suivent.

Insertion de la clé de licence

Une fois aue vous aurez recu votre clé de licence (envoyée par courriel à l'adresse indiquée lors du processus d'enregistrement), elle doit alors être insérée dans le programme. Cela permettra au programme d'être automatiquement mis à jour et d’éviter tout autre avertissement de validité de clé de licence.

Note – Le programme d’avast! doit- être téléchargé et installé avant que la clé de licence soit insérée.

Pour consulter un didacticiel vidéo montrant comment insérer la clé de licence sans démarrer le programme, cliquez ici

Alternativement, veuillez suivre les étapes decrites ci-dessous.

1. Mettez en surbrillance la clé d'enregistrement se trouvant dans l'e-mail que vous avez reçu d’avast! pour ce faire, déplacez le curseur à l'écran pour qu'il soit immédiatement à la gauche de la première lettre de la clé de licence. Appuyez et maintenez le bouton gauche de la souris et déplacez la souris vers la droite jusqu'à ce que l'ensemble de clés soit mis en évidence. Relâchez le bouton gauche de la souris puis déplacer la souris pour positionner le curseur sur la clé de licence mis en évidence. Cliquez sur le bouton droit de la souris, et dans le menu, sélectionnez "Copier".

2. Cliquez avec le bouton droit de votre souris sur l'icône d'avast! (boule bleue-(a)) qui se trouve dans la barre des tâches à côté de l'horloge et sélectionnez " A propos d'avast !..." dans le menu.

3. Dans la fenêtre qui apparait, cliquez sur le bouton "clé de licence" en bas à droite.

4. Positionnez le curseur dans la zone de la clé de licence, cliquez sur le bouton droit de la souris et dans la liste des options de menu sélectionnez "Coller". La clé de licence est maintenant entrée.

5. Cliquez sur "OK". Le programme peut maintenant continuer à être utilisé pour les 12 prochains mois à compter de la date d’enregistrement. À la fin de cette période, il sera nécessaire de vous enregistrer de nouveau afin d’obtenir une nouvelle clé de licence que vous insérez dans le programme selon la procédure ci-dessus.

Utilisation de base d'avast! antivirus

avast! antivirus offre une protection contre tous les types de programmes malveillants ainsi qu'une puissante "protection résidente", aussi communément appelée protection "à l'accès" parce que celle-ci vérifie les fichiers pour au moment de leur accès.

Normalement, la protection résidente fournit toute la protection dont vous avez besoin pour empêcher votre ordinateur d'être infecté par un virus. Une fois que le programme a été téléchargé et installé, la protection résidente fonctionne continuellement en arrière-plan et surveille toutes les parties de l'activité de votre ordinateur. Toutefois, si la protection résidente est désactivée pour une raison quelconque, ou s'il a été inactif pour une période de temps, il est possible d'effectuer un scan manuel rétrospectif (autrement connu sous le nom de scan "à la demande") de tous les fichiers se trouvant sur votre ordinateur.

avast! antivirus comprend également un écran de veille spécial qui scanne constamment votre ordinateur quand il est allumé mais non utilisé.

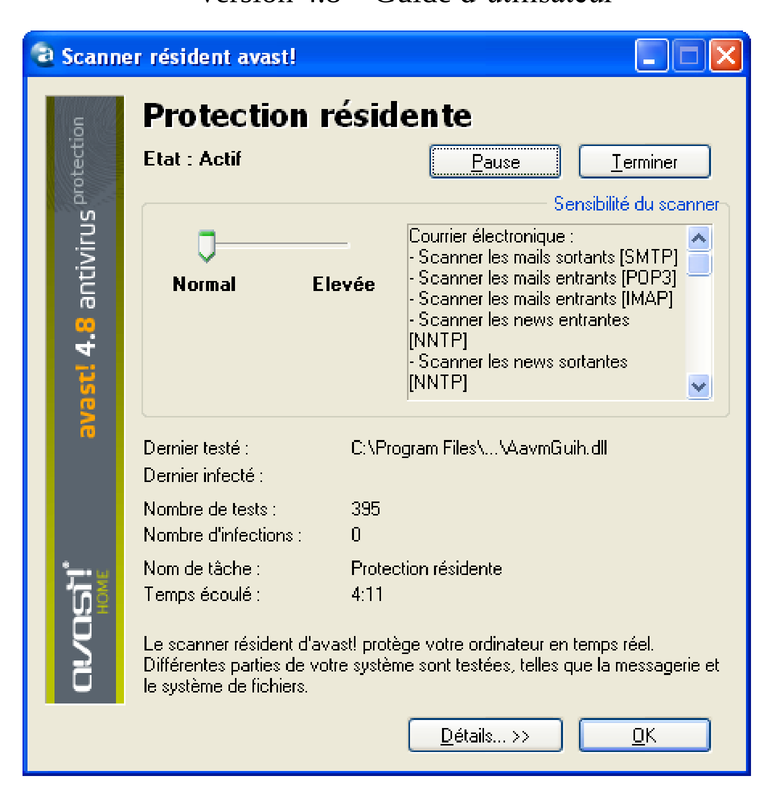
Protection Résidente "à-l'accès"

Cette partie du programme de contrôle en permanence l'ensemble de l'ordinateur et tous les programmes en cours afin de détecter toute activité suspecte (par exemple un virus), empêchant ainsi toute détérioration des fichiers sur votre ordinateur. Il fonctionne de façon totalement indépendante (il s'active automatiquement lorsque vous démarrez votre ordinateur) et si tout est OK, vous ne remarquerez même pas qu'il est en marche.

L'icône bleue "a" dans le coin inférieur droit de l'écran de l'ordinateur, à côté de l'horloge, montre l'état actuel de la protection résidente. Normalement, la présence de la boule bleue "a" indique que la protection résidente est installée et protège votre ordinateur. Si la boule bleue "a" a une ligne rouge sur elle, la protection est actuellement inactive, et votre ordinateur n'est pas protégé. Si elle a un aspect gris, cela signifie que la protection a été mise en veille - voir page suivante.

Les réglages de la protection résidente sont accessibles par un clic gauche la boule bleue "a" dans le coin inférieur droit de l'écran, ou clic droit et en sélectionnant "Gestion de la protection résidente".

La fenêtre suivante sera ensuite affichée :



Sur cette interface, vous pouvez suspendre temporairement la protection résidente en cliquant sur "Pause" ou "Terminer". Ici, deux options ont le même effet. Toutefois, la protection résidente sera automatiquement réactivée la prochaine fois que votre ordinateur est redémarré. Il s'agit simplement d'une mesure de sécurité pour assurer que votre ordinateur ne soit pas laissé accidentellement sans protection.

Vous pouvez également régler la sensibilité de la protection résidente, en cliquant sur la ligne de part et d'autre du curseur pour modifier la sensibilité à la "normale" ou "Elevée". Toutefois, la protection résidente contient plusieurs modules ou ''services'', dont chacuns de ceux-ci vise à protéger une partie différente de votre ordinateur - voir la page suivante. Toutes les modifications que vous apporterez à partir de cette interface seront applicables à tout l'ensemble des modules de la protection résidente.

La protection résidente est composé des modules ou ''services'' suivants:

Messagerie Instantanée vérifie les fichiers téléchargés par les programmes de messagerie instantanée ou "chat" tels qu'ICQ, MSN Messenger et bien d'autres. Alors que des messages instantanés en eux-mêmes ne posent pas de graves risques de sécurité en termes de virus, aujourd'hui, les applications de messagerie instantanée sont loin d'être seulement un outile de causerie: la plupart d'entre elles permettent également le partage de fichiers - qui peuvent tout à fait facilement mener aux infections virales, s'ils ne sont pas correctement surveillés.

Courrier Electronique vérifie les messages entrants et sortants des e-mails traités par des clients de messagerie autres que MS Outlook et MS Exchange, tels que Outlook Express, Eudora etc

Bouclier Réseau offre une protection contre les vers de l'Internet tels que Blaster, Sasser etc. Ceci est uniquement disponible sur les systèmes basés sur NT (Windows NT/2000/XP/Vista)

Outlook/Exchange vérifie les messages entrants et sortants des e-mails traités MS Outlook ou MS Exchange et bloquera tous les messages contenant un virus potentiel qui pourra être acceptés ou envoyés.

Bouclier P2P vérifie les fichiers téléchargés par les programmes communs P2P (partage de fichier) tel que Kazaa etc.

Blocage des Scripts (uniquement pour l'Edition Professionnelle) vérifie les scripts contenus dans les pages web que vous regardez à fin de prévenir toute infection due à la vulnérabilité de votre navigateur web.

Bouclier Standard vérifie les programmes en cours et les documents qui sont ouverts. Il permettra d'empêcher un programme infecté d'être executé ou un document infecté d'être ouvert, ceci à fin d'éviter qu'un virus soit actif et cause des dommages.

Bouclier Web protège votre ordinateur contre les virus lorsque vous êtes entrain d'utiliser l'Internet (navigation, téléchargement de fichiers, etc) et peut également bloquer l'accès à certaines pages Web. Si vous téléchargez un fichier infecté, le Bouclier Standard l'empêchera de démarrer et de causer des dommages. Toutefois, le Bouclier Web permet de détecter les virus bien avant, pendant le téléchargement du fichier, en fournissant encore plus de protection. Le Bouclier Web est compatible avec tous les principaux navigateurs web, y compris Microsoft Internet Explorer, Mozilla Firefox et Opera. Grâce à une fonctionnalité unique appelée ''Intelligent Stream Scanning'' (scan intelligent de flux), qui permet l'analyse des fichiers téléchargés presqu'en temps réel, son impact sur la vitesse de navigation est quasiment négligeable.

Il est possible d'ajuster la sensibilité de chaque module séparément. Pour régler la sensibilité pour chaque module, ou pour mettre en pause ou terminer un module spécifique, cliquez sur "Détails ...". L'interface sera alors étandue comme suit:



Dans la zone élargie, les différents modules sont affichés dans le panneau sur la gauche. La sensibilité de chaque module peut être configurée en cliquant sur le module dans la colonne de gauche, puis en cliquant sur la ligne à droite ou à gauche du curseur. Dans cette boîte, il est également possible de suspendre les différentes parties de la protection résidente, temporairement ou définitivement, en cliquant sur "Pause" ou "Terminer". Si vous cliquez sur "Pause", le module sera automatiquement réactivé la prochaine fois que vous redémarrez votre ordinateur. Si vous sélectionnez "Terminer", le programme vous demandera si vous voulez que module de reste indéfiniment désactivé, ou si il doit reprendre après le prochain redémarrage de l'ordinateur - voir page 67. Si vous cliquez sur "Oui", ce module sera désactivé, même après le redémarrage de votre ordinateur, jusqu'à ce que vous activer manuellement à nouveau.

Il existe toute une gamme d'options supplémentaires qui peuvent être sélectionnées pour chaque module, par exemple, il est possible de spécifier les types de fichiers qui doivent être scannés. Ces options sont accessibles en cliquant sur "Personnaliser" et sont décrits à la page 52 – Les réglages de la Protection Résidente.

Comment réaliser un scan manuel – l'Interface utilisateur simplifiée

Lorsque vous exécutez le programme, il vous sera présenté avec une image de l'argent gris / radio / lecteur CD qui contient tous les boutons de contrôle, de définition, de fonctionnement et le traitement des résultats d'une analyse antivirus - voir ci-dessous. Ceci est l'aspect par défaut ou «skin» du programme (cela peut être modifié en sélectionnant d'autres "skins" – voir page 30).

Initialement, le lecteur apparaît derrière une boîte qui contient les «5 points clés pour vous aider à démarrer». Cliquez sur "Plus d'informations" pour en savoir plus, puis sur "Accueil" pour revenir à l'écran principal. Les informations pertinentes sont résumées dans les pages suivantes. Vous pouvez revenir sur ces points-clés à tout moment en accédant au menu d'options (voir page suivante) et en sélectionnant "Aide d'introduction".



Dans le centre du lecteur, légèrement décalé à droite, se trouve un écran qui montre l'état actuel des informations:

- ***La version actuelle de la base de données virale*** – la base de données virale contient des détails de tous les virus connus et actuellement utilisé par le programme pour identifier les fichiers suspects.
- ***Protection Résidente*** – Ici, vous pouvez voir le niveau de sensibilité actuel.
- ***Date du dernier scan*** – la date à laquelle un scan manuel a été dernièrement effectué
- ***Base de données de Rétablissement Virale*** – elle contient des détails sur les fichiers installés sur votre ordinateur et est utilisée pour les réparer s'ils sont endommagés par un virus. La date indiquée est la date à laquelle la base de données de Rétablissement Virale a été mise à jour.

- ***Mises à jour Automatiques*** – cela montre le statut de mise à jour concernant à la fois la base de données virale et le programme lui-même - pour changer le statut de mise à jour, cliquez sur la situation actuelle sur le côté droit de la fenêtre - voir page 37.

De l'autre côté de l'écran on peut voir trois boutons de contrôle:

- **En haut à gauche** – Ce bouton va ouvrir la Zone de Quarantaine. Pour les informations concernant la manipulation des fichiers de la zone de quarantaine, voir page 48.

- **Centre gauche** – En cliquant sur ce bouton il vous sera affiche un barre avec un curseur qui peut être utilisé pour changer la sensibilité de la protection résidente. Cliquez sur le curseur et le déplacer vers la gauche ou la droite pour diminuer ou augmenter la sensibilité. Note – le changement du niveau de sensibilité ici aura affectera tous les modules de la protection résidente. Pour ajuster les modules séparément, voir page 22

- **En bas à gauche** – En cliquant sur ce bouton, ou en cliquant sur la situation actuelle dans la fenêtre d'affichage, la base de données de virus sera mise à jour.

- **La base de données de Rétablissement virale** peut être également mise à jour par un clic droit sur la boule bleue "i" dans le coin inférieur droit de votre écran d'ordinateur, et en sélectionnant une des options pour "Générer VRDB".

- **Les trois boutons de droite** sont utilisés pour définir les zones à scanner – toute combinaison des disques durs locaux, les médias amovibles (disquettes, CD etc) et les dossiers sélectionnés - voir la page suivante.

- Le button **DEMARRER** – cliquez sur ce bouton pour demarrer ou reprendre le scan de la (des) zone(s) sélectionnée(s). Ce bouton change alors à un bouton de **PAUSE**.

- Le button **PAUSE** – En cliquant sur ce bouton, le scan sera temporairement arrêté.

- Le button **STOP**. Cliquez sur ce bouton pour terminer le scan.

EJECT - En cliquant sur le bouton de flèche dans le coin supérieur gauche du lecteur, vous verez le **MENU** des **OPTIONS**. Les options de menu sont également accessibles en cliquant avec le bouton droit de votre souris avec le curseur positionné n'importe où sur le lecteur.

Lorsque vous utilisez le programme sans "skin" (voir page 30), les options du menu sont accessibles en cliquant sur "Outils" ou "Réglages" en haut de l'écran.

Certaines options de menu peuvent être consultées sans le démarrage du programme, par un clic droit sur la boule bleue «a» dans le coin inférieur droit de l'écran de l'ordinateur.

Sélection manuelle des zones à scanner

Avant de lancer un scan, vous devez choisir les fichiers que vous souhaitez scanner.

- ***Analyse des disques locaux***

  Si vous voulez simplement scanner tout sur votre ordinateur (tous les fichiers sur tous les disques durs), cliquez sur le bouton en haut à droite. L'écran avec les informations sur le statut est désormais remplacé par un nouveau fond d'écran - voir ci-dessous. Pour revenir à l'état des informations, cliquez avec le bouton droit de votre souris sur le lecteur et sélectionner "information sur le statut".



Sur l'écran, vous allez maintenant voir la rubrique "Scan disques durs locaux" et a changé le statut de "Off" à "On".

Vous verrez aussi qu'une autre boîte est apparue au-dessus du lecteur. Ceci peut être utilisé pour régler la sensibilité de l'analyse. Par un clic gauche sur le curseur et la tenue de votre bouton de la souris, vous pouvez déplacer le curseur vers la gauche pour réduire la sensibilité, ou vers la droite, ce qui augmente la sensibilité. Dans cette case, vous pouvez aussi choisir si vous voulez scanner les fichiers archives. Ces options sont décrites plus en détail dans la section suivante.

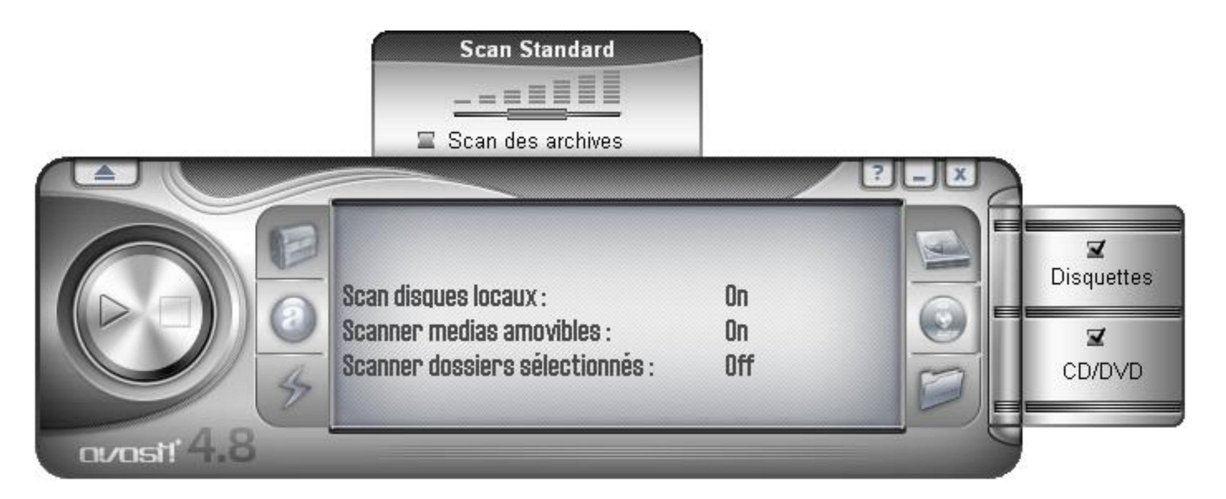
- ***Scanner les medias amovibles***

  Si vous souhaitez scanner le contenu de certains supports amovibles, par exemple, disquettes ou CD / DVD, cliquez sur le bouton de centre-droit.

  Cliquez sur ce bouton pour modifier le statut de "Scanner medias amovibles" du "Off" à "On".

  Deux boîtes vont également apparaître à la droite du lecteur avec des cases qui peuvent être cochées ou non pour indiquer quel type de support amovible doit être scanné (d'autres medias magnétiques et magnéto-optiques, tels que les disques ZIP, également considérés comme des disquettes).

  La boite au-dessus du lecteur sera aussi affichée, à cet endroit, vous pouvez spécifier la sensibilité de l'analyse et si les fichiers d'archives devraient aussi être scannés.



- ***Scanner des dossiers sélectionnés***

  La dernière option est le bouton en bas à droite. Vous devez cliquer sur ce bouton si vous souhaitez définir que seulement certains dossiers devraient être scannés. Après avoir cliqué sur ce bouton, une liste de tous les dossiers de votre ordinateur sera affichée à partir de laquelle vous pouvez sélectionner les dossiers que vous souhaitez scanner. Cette configuration offre donc plus de souplesse, mais exige que l'utilisateur fasse les paramètres précis de ce qui doit être scanné.

  Vous pouvez régler la sensibilité de l'analyse et préciser si les fichiers d'archives devraient aussi être scannés de la même manière que pour les autres zones.

  Il est possible de combiner plus d'un type de scan, il est par exemple très bien de lancer le scan de l'ensemble de vos disques durs et amovibles en cliquant à la fois les boutons disques durs locaux et medias amovibles.

Réglage de la sensibilité du scan et exécution du scan

Lors de la définition de la (des) zone(s) à scanner, vous pouvez également régler la sensibilité de l'analyse et si oui ou non l'analyse du contenu des archives c'est-à-dire les fichiers avec les noms de fichiers se terminant par .Zip, .Rar, ace, .ACJ etc . Pour inclure ces fichiers, en premier lieu sélectionnez les zones que vous souhaitez analyser (voir ci-dessus) puis cliquez sur la case à cocher "scan des archives" qui apparaît au-dessus du lecteur. La sensibilité est réglée en déplaçant le curseur vers la gauche ou la droite. Vous pouvez choisir entre trois niveaux prédéfinis.

- **Scan rapide**. Cette analyse, comme son nom l'indique, est très rapide comme les dossiers sont examinés en fonction de leurs noms de fichiers, et seulement ceux qui sont considérés comme potentiellement dangéreux sont effectivement analysés. Ce type d'analyse peut parfois conduire à des fichiers qui contiennent des virus d'être négligés, mais il est généralement suffisant.

- **Scan Normal**. Dans ce type de scan, les fichiers sont analysés en fonction de leur contenu (et non en fonction de leurs noms, comme dans le Scan Rapide). Toutefois, seul les parties "dangereux" des fichiers sont analysées, et non la totalité des fichiers. Ce type de scan peut également conduire à un virus non détecté, mais il est beaucoup plus efficace que le Scan rapide.

- **Scan Minutieux**. Dans ce type d'analyser tous les fichiers sont analysés dans leur intégralité pour rechercher toutes les infections énumérées dans la base de données. Ce type d'analyse est le plus fiable, mais prend beaucoup plus de temps d'exécution par rapport à un scan rapide ou normal.

Après avoir sélectionné les options de scan, tout ce que vous avez à faire est de lancer l'analyse. Pour ce faire, cliquez sur le bouton de lecture (flèche pointant à droite) sur le côté gauche du lecteur.

Methode Alternative

Vous pouvez aussi définir la/les zone(s) à scanner en ouvrant le menu des options et en cliquant sur "Démarrer le scan" et ensuite "Zone à analyser". Une fois que vous avez sélectionné la zone à analyser, vous pouvez aussi spécifier si les archives devraient être incluses en sélectionnant "Scan des archives".

En cliquant sur "Niveau d'analyse" vous pouvez aussi spécifier si le scan devrait être un scan Rapide, un scan standard, ou un scan minutieux commme décrit plus haut.

Lancement d’une analyse et traitement des resultats

Après avoir cliqué sur le bouton de lecture, ou en sélectionnant "Démarrer le scan - Entrée" dans le menu des options, le programme commence à analyser les zones sélectionnées. Ce processus peut prendre un certain temps, selon le nombre et la taille des fichiers analyses et de la vitesse de votre ordinateur. N'oubliez pas que même si l'option Scan minutieux prend le plus de temps, c'est le plus efficace.

Une fois le programme lancé, vous pouvez travailler avec d'autres fichiers ou programmes sur votre ordinateur, même si l'analyse est en cours. Pour ce faire, il est recommandé de réduire le programme d’avast! afin qu'il s'exécute en arrière-plan. Sinon, vous constaterez que votre ordinateur devient très lent (l’analyse pour la recherche de virus est une tâche exigeante). Pour envoyer le scan en arrière-plan, il suffit de cliquer sur le bouton de réduction (_) dans le coin supérieur droit du lecteur pendant que l’analyse est en cours d'exécution, et il disparaîtra de l'écran. Pour le ramener, il suffit de cliquer sur le bouton "avast!" qui se trouve dans la barre horizontale en bas de l'écran.

Lorsque l'analyse est terminée, et si aucun virus n’a été détecté, la fenêtre du lecteur affiche les informations de base du scan, tels que le nombre de dossiers et de fichiers analysés, le temps d'exécution etc

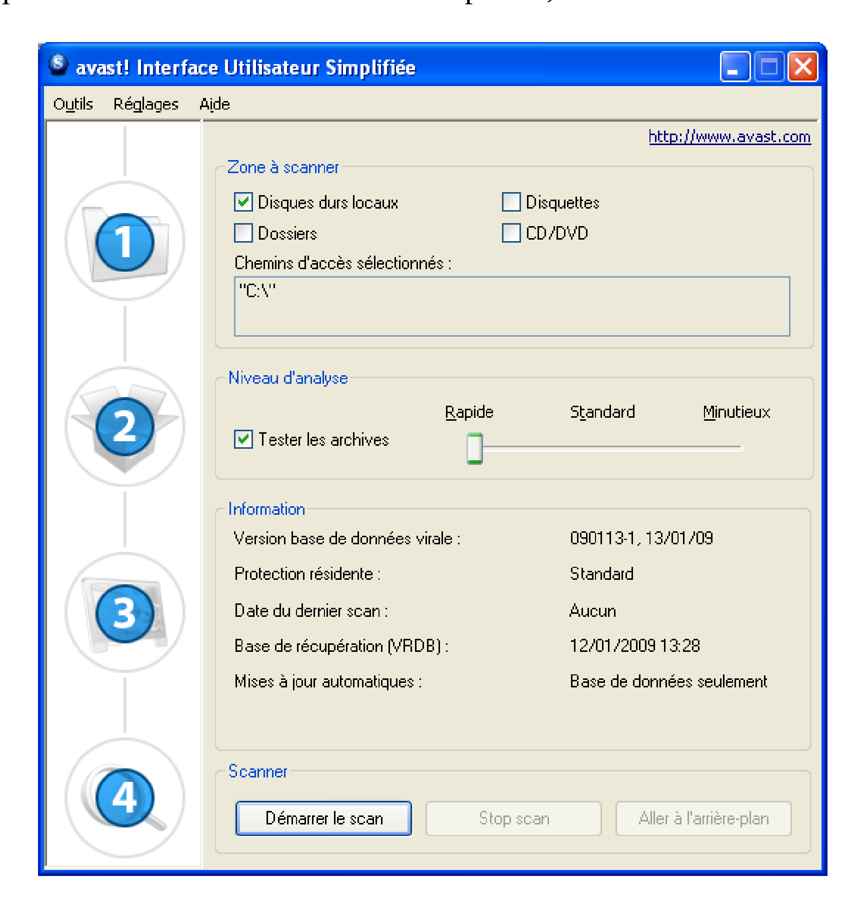


Si un virus est trouvé, le programme vous demandera quoi faire avec le(s) fichier(s) infecté(s). Il existe un certain nombre d'options, par exemple, pour déplacer le fichier vers la zone de quarantaine, pour le supprimer, pour le renommer ou le déplacer, ou, si possible pour le réparer. Vous pouvez aussi tout simplement laisser le fichier intact, toutefois, cette option peut entrainer la propagation du virus et causer d'autres dommages. Ces options sont décrites plus en détail dans la section "Que faire lorsqu’un virus est détecté".

Changer l'apparence de l'Interface Utilisateur Simplifiée

Si vous utilisez l'interface utilisateur Simplifiée, il est possible de sélectionner les différents programmes d'habillage. Trois skins (fichiers d'apparences) sont proposés a la base et d'autres peuvent être téléchargés à partir d'Internet si besoin est - un clic droit sur le lecteur d'avast! et à partir des options de menu, cliquez sur ‘‘choisir le thème’’, puis sur le lien "D'autres thèmes sur notre serveur web!". Alternativement, si vous souhaitez utiliser le programme sans aucun thème, sélectionnez "Réglages" dans le menu d'options, puis décochez la case "Activer les thèmes pour l'interface utilisateur simplifiée". La prochaine fois que vous démarrez le programme, les options seront affichées dans leur format de base. Pour restaurer le thème, cliquez sur "Réglages" et encore sur "Réglages", et enfin re-cocher la case "Activer les thèmes pour l'interface utilisateur simplifiée". Le thème sera restauré la prochaine fois que vous lancez le programme.

L'apparence de l'interface utilisateur simplifiée, sans le thème:



La ou les zone(s) à être analysée(s) et le type de scan sont alors réglés en cochant les cases appropriées. Si vous souhaitez analyser uniquement des dossiers spécifiques, en cochant la case "Dossiers", il s'ouvrira une nouvelle fenêtre contenant la liste de tous les dossiers de votre ordinateur. Pour sélectionner un dossier, il suffit de cocher la case appropriée, et elle apparaîttra dans la section ci-dessus "Chemins d'accès Sélectionnés".

Vous pouvez régler la sensibilité de l'analyse en déplaçant le curseur vers la position souhaitée et si vous voulez que les archives soient scannées, cliquez sur "Tester les archives".

Après avoir lancé le scan, vous pouvez continuer à utiliser votre ordinateur pour d'autres tâches en cliquant sur "Aller à l’arrière plan".

Vous pouvez également régler la sensibilité de la protection résidente en cliquant sur "Réglages" et ensuite sur "protection résidente". Vous pouvez utiliser le curseur pour modifier la sensibilité à "Standard" ou "Elevée" ou vous pouvez désactiver complètement la protection résidente, en mettant le curseur sur "Désactivé". Cependant, comme décrit précédemment, toutes les modifications que vous effectuez ici s'appliquent également à tous les modules de la protection résidente. Pour ajuster la sensibilité des modules individuellement, voir page 22.

Vous pouvez accéder à d'autres options telles que la zone de quarantaine et la base de données virale en cliquant sur "Outils" et sélectionnant l'option désirée parmi celles qui sont disponibles. Celles-ci, et toutes les autres caractéristiques sont décrites en détail plus loin dans ce guide de l'utilisateur.

L'état actuel des informations est présenté dans la moitié inférieure de l'écran, et ceci est décrit dans la section précédente.

Que faire lorsqu’un virus est trouvé

Si le programme detecté un fichier souspicieux, le scan sera interrompu à ce point et la fenêtre suivante s’affirera en vous demandant comment vous voulez le traiter:

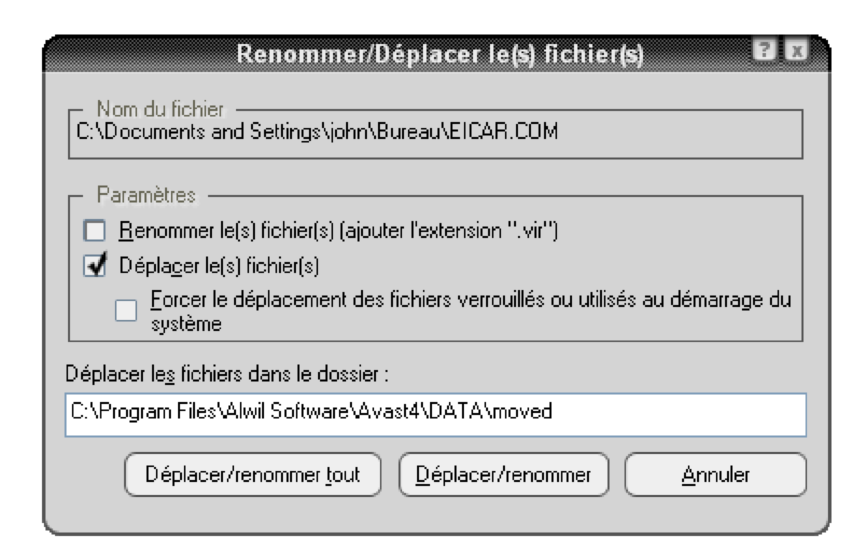


En cliquant sur "Continuer" signifie qu’aucunes mesures ne seront prises maintenant par rapport au fichier identifié et cela sera reporté à la fin du scan dans la liste des résultats d’analyse - voir la page 36. En cliquant sur "Stop" vous mettrez fin à l'analyse à ce point.

Si un virus est détecté par l'un des modules résidents, par exemple en essayant d’ouvrir un fichier infecté, ou par l'économiseur d'écran, l'écran sera légèrement différent – les boutons "Continue" et "Stop" seront remplacés par un seul bouton "Ne rien Faire". Si vous cliquez sur ce bouton de manière à ce qu'aucune mesure ne soit prise à ce moment, le fichier infecté restera où il est, mais le virus ne sera pas activé.

Alternativement, si vous voulez prendre une action maintenant, il y a quatre options possibles.

Option 1: Déplacez le fichier infecté vers un autre dossier sur votre ordinateur. Dans le même temps, vous aurez la possibilité de le renommer. En cliquant sur "Déplacer / Renommer" affichera la fenêtre suivant la case "Déplacer le fichier (s)" déjà cochée.



Dans la partie blanche de l'écran, il est possible de spécifier l'endroit où vous voulez que le fichier suspect soit déplacé. Le programme sélectionne automatiquement un dossier de destination approprié, ou vous pouvez spécifier un autre.

Si vous cochez la case "Renommer le(s) fichier(s)....", cela va ajouter l'extension ".Vir" à la fin du nom du fichier pour l'identifier comme étant potentiellement dangereux, afin que vous ne l’exécutiez accidentellement, et qu’il n'infecte votre ordinateur et cause des dommages.

S'il n'est pas possible de déplacer le fichier en ce moment, par exemple car il est utilisé par un autre programme, cochez la case "Forcer le déplacement des fichiers verouillés ou utilisés au démarrage du système" cela fera que le fichier sera déplacé automatiquement vers la destination choisie la prochaine fois que l'ordinateur est redémarré.

Note - dans le cas où un ***fichier système*** est infecté c'est-à-dire un fichier qui est utilisé pour exécuter un programme clé, le déplacement du fichier pourrait aboutir à une erreur la prochaine fois que votre ordinateur tente d'exécuter le programme. Toutefois, si le fichier est placé dans la zone de quarantaine, il y sera protégé et ne pourra causer de dommages à vos autres fichiers. A partir de la, il peut éventuellement être réparé avant de le remettre à son emplacement d'origine - voir page 8

Option 2: Supprimer le fichier – cliquer sur "Supprimer" entrainera la fenêtre suivante:



Cela dépend de quelle version de Windows vous utilisez, il y a deux manières par lesquelles le fichier peut être supprimé.

- ***Supprimer le(s) fichier(s) et les mettre dans la corbeille***
  ceci va déplacer le(s) fichier(s) vers la corbeille mais ne les supprimera pas de manière permanente. Ils peuvent être plutard restaurés. Cette option peut ne pas être disponible dans certaines versions de Windows.

- ***Supprimer le(s) fichier(s) de manière permanente***
  cela permettra de supprimer le(s) fichier(s) de votre ordinateur de façon permanente sans aucune possibilité de les restaurer ultérieurement. Toutefois, cela ne fera que supprimer le fichier infecté. Certains virus installent de nouveaux fichiers sur votre ordinateur et ces fichiers, en eux-mêmes ne contiennent pas de virus, ils ne seront pas détectés comme suspects. Bien que ces fichiers prennent de l'espace sur votre ordinateur, il ne devrait pas présenter de risque de sécurité.

Si un virus est détecté, et peut être complètement enlevée par le nettoyeur de virus incorpore, notamment en éliminant les nouveaux fichiers créés par le virus, un bouton supplémentaire - "supprimer complètement le virus du système" - apparaît dans la boîte de message d'avertissement. Si cette option est disponible, il est recommandé de l'utiliser.

S'il n'est pas possible de supprimer le fichier en ce moment, par exemple car il est utilisé par un autre programme, cochez la case "***Si nécessaire, supprimer le(s) fichier (s) au prochain démarrage du système***" entrainera la suppression automatique du fichier la prochaine fois que l'ordinateur est redémarré. Puis cliquez sur "Supprimer" de nouveau pour confirmer la suppression.

Note - dans le cas où un ***fichier système*** est infecté c'est-à-dire un fichier qui est utilisé pour exécuter un programme clé, le supprimer pourrait aboutir à une erreur la prochaine fois que votre ordinateur tente d'exécuter le programme. Avant de supprimer le fichier, vous devez donc être sûr que le fichier infecté n'est pas un fichier système, ou que vous êtes en mesure de le remplacer par un fichier propre, par exemple à partir d'une sauvegarde.
Si vous n'êtes pas sûr, il est recommandé de déplacer le fichier dans la zone de quarantaine. A cet endroit, il sera protégé et il ne pourra causer aucun dommage à vos autres fichiers et

aussi d'où il pourra éventuellement être réparé avant de le remettre dans son emplacement d'origine - voir page 8

Option 3: Réparer le fichier.

Un clic sur "Réparer" vous affichera la fenêtre suivante:



Si vous cliquez encore sur "Réparer", le programme va essayer de restaurer les fichiers infectés afin de les ramener à leur état original.

Pour réparer un fichier, le programme se référera à la ***base de données de rétablissement de virus***. S'il ya suffisamment de renseignements sur le programme dans la base de données, il ya de bonnes chances qu'il puisse être réparé. Note - seuls les fichiers qui ont été physiquement modifiés par un virus peuvent-être réparés. Si de nouveaux fichiers ont été créés, ils demeureront, sauf s'ils peuvent être supprimés par le programme de nettoyage de virus - voir l'option 2.

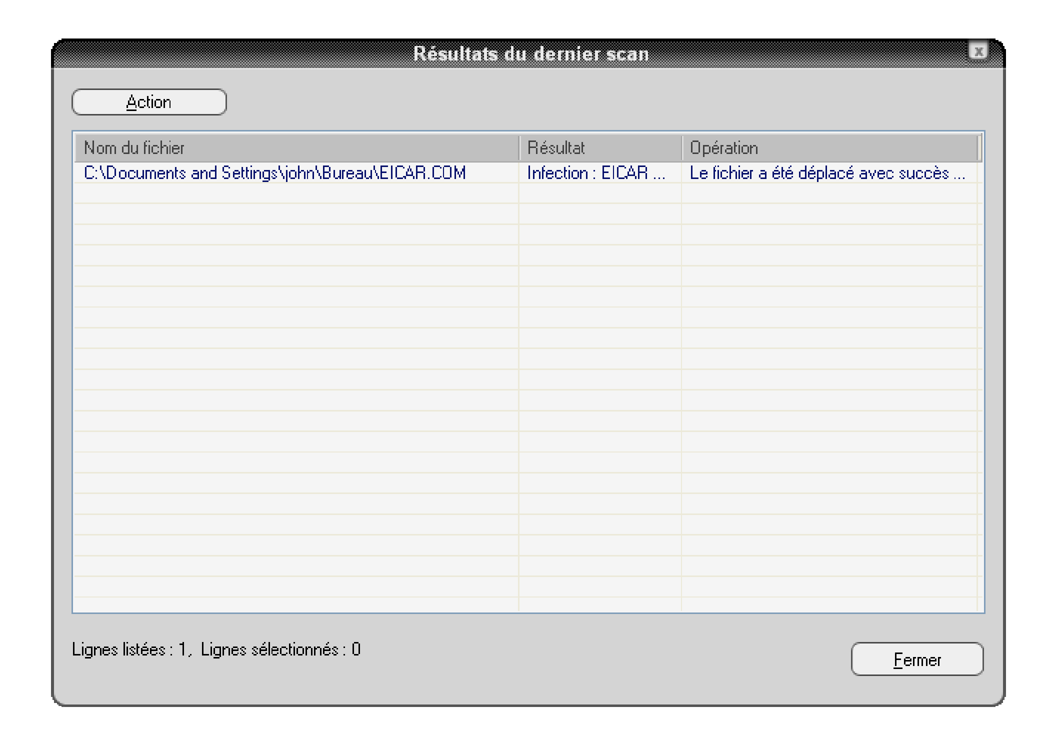
S'il n'ya pas d'informations dans la base de données, la réparation peut encore être possible, mais le recouvrement intégral est moins sûr. Il est donc très important que la base de données soit continuellement mise à jour - pour mettre à jour la base de données de rétablissement de virus, cliquez avec le bouton droit sur la boule bleue "i" dans le coin inférieur droit de votre écran d'ordinateur et sélectionnez l'option "Générer la VRDB". La base de données sera mise à jour avec les détails de tous les nouveaux programmes installés sur votre ordinateur depuis la dernière mise à jour.

Option 4: L'OPTION **RECOMMANDEE** est de déplacer le fichier vers la Zone de Quarantaine.

Note - dans le cas où un ***fichier système*** est infecté c'est-à-dire un fichier qui est utilisé pour exécuter un programme essentiel, le déplacement du fichier pourrait aboutir à une erreur la prochaine fois que votre ordinateur tente d'exécuter le programme. Toutefois, si le fichier est placé dans la Zone de Quarantaine, il sera protégé à cet endroit, il ne pourra causer de dommages aux autres fichiers et il pourra être éventuellement réparé avant de le remettre à son emplacement d'origine - voir page 8

Résultats du dernier scan

Une fois que vous avez spécifié la façon dont vous voulez traiter avec le fichier sélectionné, l’analyse reprend automatiquement. Si d'autres fichiers suspects sont identifiés, l'analyse s'arrête à nouveau (à moins que l'option "Supprimer tout" ait été choisie lors d'un scan "à la demande") et le processus est répété. Lorsque l'analyse est terminée, les resultats sont présentés avec les détails des mesures prises à l'égard de chaque fichier suspect identifié voir ci-dessous.



Si vous avez choisi de ne prendre aucune action au cours du processus d’analyse par rapport à tout fichier particulier, ce fichier sera répertorié dans l'analyse des résultats, mais la colonne "Opération" sera vide.

Pour traiter le fichier maintenant, cliquez d'abord sur le nom du fichier dans la table, puis cliquez sur "Action" dans le coin supérieur gauche et vous verrez la liste des options, comme décrit dans les pages précédentes. Les mesures prises seront ensuite affichées dans la colonne "Opération".
Une fois que vous êtes convaincu que tous les fichiers suspects ont été traitées, cliquez sur "Fermer" pour mettre fin au processus d’analyse. Pour visualiser les résultats de nouveau, ouvrez le menu des options et sélectionnez l'option "Derniers résultats…".

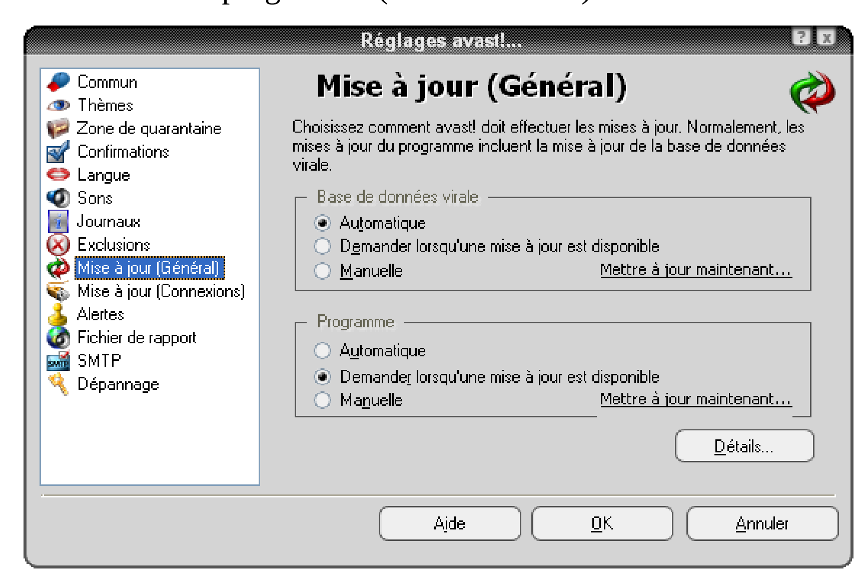
Note: Si vous fermez le programme d’avast!, l’option "Derniers résultats…" ne sera pas disponible et vous ne serez pas en mesure d'afficher les résultats de la dernière analyse la prochaine fois que vous lancez le programme. Cette option sera de nouveau disponible que si vous lancez une nouvelle analyse. Toutefois, les détails de tout virus ou d'erreurs détectées sont enregistrées et peuvent être vus par l'ouverture du visualiseur de journaux log - voir page 50.

Fonctionnalités avancées

Réglage des mises à jour automatiques

Tout programme d'anti-virus est aussi bon que sa base de données de définitions de virus connus, c'est pourquoi il est important de mettre régulièrement à jour à la fois le programme et la base de virus.

Vous pouvez choisir si le programme et la base de virus seront mises à jour automatiquement ou manuellement, ou seulement en suivant la notification selon laquelle une mise à jour est disponible pour avast! Pour changer l'état, vous pouvez soit cliquer sur le statut actuel (par exemple, "uniquement la base de données") au niveau de l'écran du lecteur d'avast!, ou simplement ouvrir le menu des options , sélectionnez "Réglages…", puis "Mise à jour (Général)". Ensuite, il suffit de cliquer sur le statut souhaité de la base de données de virus et du programme (voir ci-dessous).



Cliquez sur "OK" et l'état dans la fenêtre du lecteur sera mise à jour comme ce qui suit:

- **ON** si "Automatique" est sélectionné pour les deux, la base de données virale et le programme
- **PROGRAMME SEULEMENT** si "Automatique" est sélectionné pour uniquement pour le programme
- **BASE DE DONNEE…** si "Automatique" est sélectionné pour uniquement pour la base de données virale
- **OFF** si "Automatique" n'est pas sélectionné pour pour les deux, ni pour la base de données virale et ni pour le programme

Pour mettre **manuellement** à jour le programme ou la base de données de virus, accédez au menu des options (voir page 25) et sélectionnez l'option "Mise à jour".

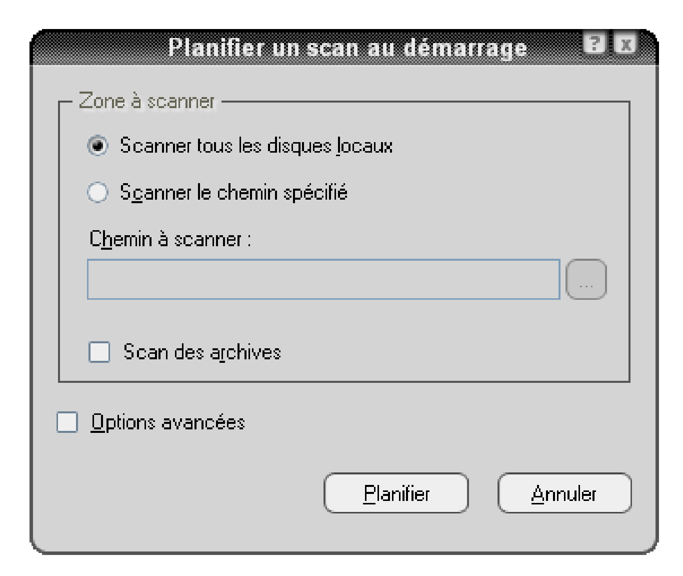
- Pour la base de données de virus, sélectionnez **Mise à jour de la base virale**
- Pour mettre à jour le programme d'avast!, sélectionnez **Mise à jour du Programme**

Comment planifier un scan au démarrage

(Uniquement pour les versions 32 bit de Windows NT/2000/XP/Vista)

Il est possible de programmer une analyse qui sera effectuée automatiquement lors du redémarrage de l'ordinateur, c'est-à-dire que le scan s'exécutera bien avant que le système d'exploitation ne soit actif. Ceci est utile si vous soupçonnez la présence d'un virus sur votre ordinateur parcequ'un tel scan permettra au virus d'être détecté avant qu'il ne soit activé, et donc avant qu'il n'ait eu la chance de faire des dégâts.

Pour planifier un scan au démarrage, accédez au menu des options (voir page 25) et cliquez sur "Planifier un scan au démarrage ". La fenêtre suivante sera ensuite affichée:



Ici, vous pouvez choisir si vous souhaitez analyser tous les disques ou uniquement certaines zones. Pour analyser uniquement les zones choisies, cliquez sur "Chemin à scanner" et tapez le nom du chemin d'accès dans la case prévue, ou cliquez sur le carré à droite pour rechercher la zone que vous souhaitez analyser. Lorsque vous avez trouvé la zone que vous souhaitez scanner, cliquez sur celle-ci et le nom du chemin d'accès sera automatiquement copié dans la case prévue.

Si vous voulez inclure les archives, il suffit de cocher la case "Scan des archives".
En cochant la case "Options avancées", vous pouvez indiquer ce qui doit être fait avec les fichiers infectés. Vous pouvez choisir parmi l'une des options suivantes:

- Supprimer le fichier infecté
- Déplacer le fichier infecté
- Déplacer le fichier infecté dans la Quarantaine
- Ignorer le fichier infecté
- Réparer le fichier infecté

La sélection de "Déplacer le fichier infecté" permettra à avast! de déplacer tout fichier suspect vers le dossier C:\Program Files\Alwil Software\Avast4\DATA\moved. L'extension ".Vir" sera également ajoutée à la fin du nom du fichier afin de l'identifier comme fichier suspect pour ne pas l’exécuter accidentellement, ce qui infectera votre ordinateur et causera des dommages à vos fichiers.

Si vous choisissez une des options pour supprimer ou de déplacer les fichiers infectés, il vous sera demandé de confirmer ce que vous voulez faire avec n'importe quels **fichiers système** infectés.

Les fichiers Système sont des fichiers qui sont utilisés par votre ordinateur d'exécuter vos programmes et la suppression ou le déplacement de l’un d’entre eux pourraient avoir des conséquences graves. Vous êtes donc invité à confirmer si vous souhaitez:

• Permettre de supprimer ou de déplacer, ou
• ignorer supprimer ou déplacer les fichiers système

La se sélection de "Ignorer supprimer ou de déplacer" permettra d'éviter d'éventuels problèmes de fonctionnement, cependant, votre ordinateur courira toujours des risques d’infection. L'action recommandée est donc de déplacer tous les fichiers suspects dans la zone de quarantaine. Une fois déplacés dans la quarantaine, ils ne peuvent pas causer des dommages à vos autres fichiers. Vous pouvez ensuite traiter les fichiers infectés comme décrit à la page 48, par exemple, ils peuvent être supprimés, si vous êtes sûr qu'il est sans risque de le faire, ils peuvent être déplacés vers leur emplacement d'origine, ou ils peuvent être simplement stockés jusqu'à ce que vous décidez ce qu'il faut faire.

Une fois que vous avez confirmé la façon dont les fichiers infectés seront traités, cliquez sur "Planifier" et le message suivant s'affichera:



Cliquez sur “Oui” pour redémarrer votre ordinateur et lancez le scan au démarrage maintenant, ou sur "Non" et le scan sera effectué automatiquement la prochaine fois que vous redémarrez votre ordinateur.

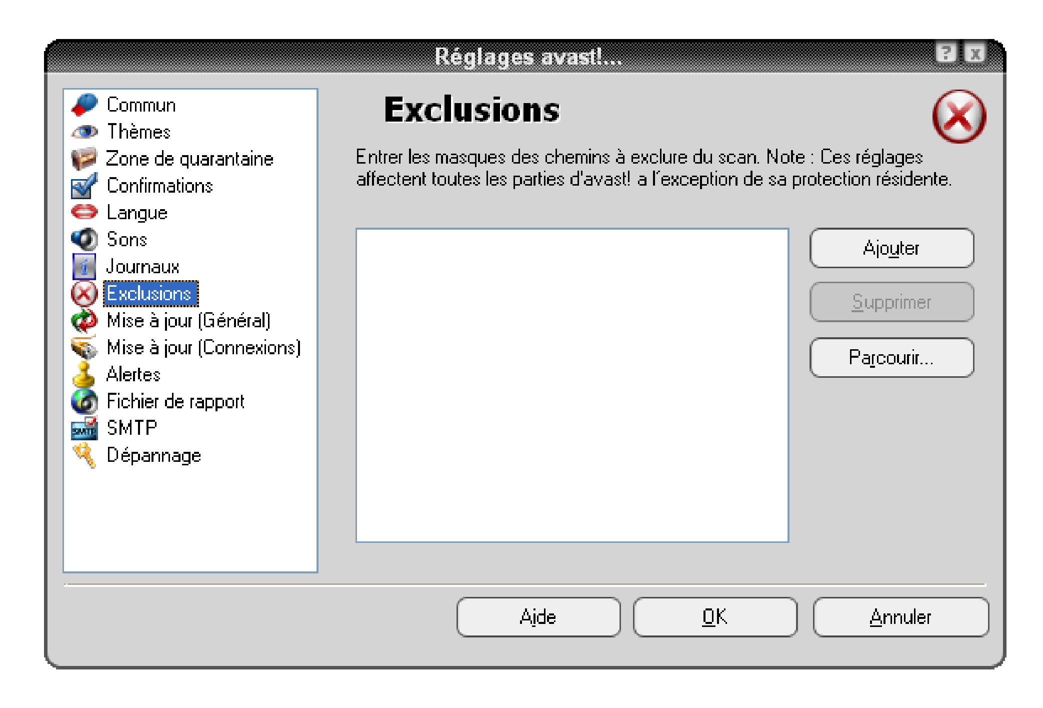
Exclusion de certains fichiers pendant l'analyse

Il est possible d'exclure certaines zones, ou même des fichiers spécifiques pendant le scan, ce qui signifie qu'ils ne seront pas vérifiés pendant toute analyse. Ceci peut-être utile dans plusieurs cas:

- **Pour éviter les fausses alarmes .** Si le programme fait état d'une infection virale dans un fichier et vous êtes sûr que c'est une fausse alerte, vous pouvez exclure le fichier de l'analyse pour éviter d'autres fausses alarmes. S'il vous plaît renseignez avast! par rapport à de tels fichiers afin que le problème soit résolu.

- **Pour accélérer le traitement .** Si vous avez un dossier sur votre disque dur qui contient uniquement des images par exemple, vous pouvez l'exclure de l'analyse en l'ajoutant à la liste des exclusions, ce qui réduira le temps consacré au scan.

  Gardez à l'esprit que ces exclusions concernent toutes les analyses, à l'exception de la protection résidente. Pour exclure certains fichiers ou dossiers de l'analyse, il vous suffit de cliquer sur "Réglages" dans le menu des options (voir page 25) puis sur "Exclusions" et l'écran suivant s'affichera:



Pour exclure un dossier ou un fichier, cliquez sur parcourir et cochez la case relative au dossier ou au fichier à exclure. Sinon, cliquez sur "Ajouter" et tapez manuellement l'emplacement du dossier ou le fichier dans la boîte Exclusions. Si vous voulez exclure un dossier, y compris tous ses sous-dossiers, il est nécessaire d'ajouter "*" à la fin du nom du dossier, par exemple C:\Windows*. Pour supprimer un dossier ou un fichier à partir de la liste des exclusions, cliquez une fois pour le mettre en surbrillance, puis cliquez sur "Supprimer"

Comment créer un rapport des résultats d'analyse

Vous pouvez créer un fichier permanent du résulat de chaque analyse par la création d'un rapport que vous pouvez ensuite visualiser plus tard. Pour créer un rapport, tout d'abord accéder au menu des options tel que décrit à la page 25 et sélectionnez "Réglages". Ensuite cliquez sur "Fichier de rapport" et dans l'écran suivant, cochez la case "Créer fichier de rapport", comme indiqué ci-dessous.



Si vous voulez créer un nouveau rapport après chaque analyse, et vous ne souhaitez pas conserver un enregistrement de tous les résultats des analyses précédentes, cochez la case "Ecraser existant". Si cette case n'est pas cochée, les résultats de chaque analyse seront ajoutés à la fin du rapport précédent.

Vous pouvez également choisir l'endroit où vous souhaitez que le rapport soit sauvegardé - dans le dossier standard du programme, que le programme attribue automatiquement, ou dans un nouvel endroit où vous pouvez spécifier en cliquant sur "Dossier personnalisé du programme" et d'entrer l'emplacement du dossier.

Ensuite, vous pouvez spécifier quelles informations seront contenues dans le rapport:

- Début de tâche - la date et l'heure auxquelles l'analye a été lancée
- Fin de tâche - la date et l'heure auxquelles l'analyse a été completée
- Fichiers OK - les fichiers qui ont été scannés sans détecter tout élément suspect. Si tous les lecteurs locaux sont scannés, en cochant cette case, cela produira un très long rapport, peut-être de plusieurs milliers de lignes. Il est donc recommandé de cocher cette case seulement si vous avez l'intention de procéder à une analyse limitée, et seulement si vous voulez que tous les fichiers sains soient également enumérés comme tous les autres fichiers problématiques.
- Erreurs matérielles se produisent lorsque le programme détecte quelque chose qui ne devrait normalement pas être attendu. Ce sont des erreurs qui ont généralement besoin d'une enquête complémentaire.

- Erreurs Logicielles sont moins graves que les erreurs materielles et, en général, elles se rapportent à des fichiers qui n'ont pas pu être analysés comme ils sont ouverts et utilisés par une autre application.
- Fichiers ignorés sont des fichiers qui ne sont pas scannés sur la base des paramètres d'analyse. Par exemple, dans une analyse rapide, les fichiers sont analysés en fonction de leur extension. Les fichiers avec des extensions qui ne sont pas considérées comme dangereuses, ne sont pas analysés. Tous les fichiers spécifiquement exclus de l'analyse seront également indiqués comme fichiers ignorés.
- les fichiers infectés - ces fichiers qui contiennent potentiellement des virus

  Enfin, vous pouvez spécifier si le rapport doit être sous la forme d'un fichier texte ou un fichier XML. Après avoir exécuté l'analyse, il y aura une nouvelle ligne dans la fenêtre des informations sur le statut - "Voir le rapport du dernier scan", comme indiqué ci-dessous.



En cliquant sur "Voir le rapport du dernier scan" il vous sera affiché le rapport dans le format de fichier spécifié. Sinon, ouvrez le menu des options (voir page 25) et cliquez sur "Voir les rapports de scan"

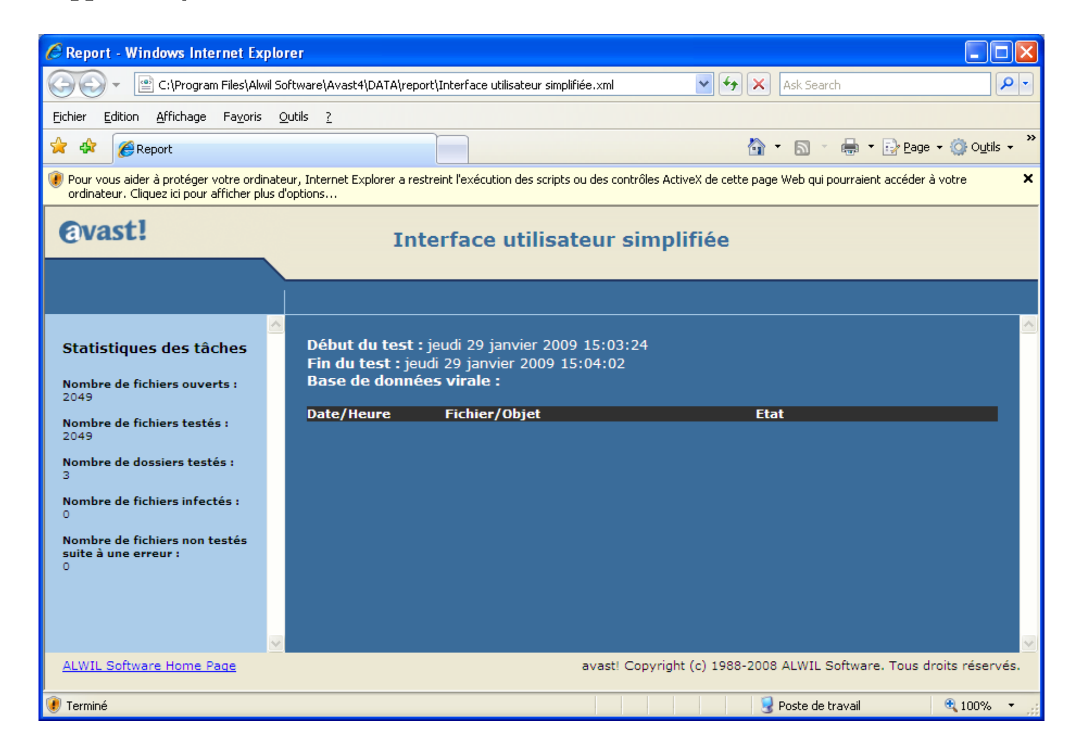
Rapport au format text:

```
*
* Rapport avast!
* Ce fichier est généré automatiquement
*
* Tâche utilisée 'Interface utilisateur simplifiée'
* Débuté le jeudi 29 janvier 2009 14:58:37
* VPS : 090128-0, 28/01/2009
*

Fichiers infectés : 0
Total des fichiers : 2049
Total des dossiers : 3
Taille totale : 515,7 MB

*
* Tâche terminée : jeudi 29 janvier 2009 14:59:29
* Programme était en exécution 52 seconde(s)
*
```

Rapport au format XML



Les rapports des analyses précédentes sont stockés dans le dossier standard du programme ou dans un dossier personnalisé spécifié lors de la création du rapport - voir page précédente.

Si vous avez spécifié le format de texte et vous n'avez pas coché la case "Ecraser existant", vous serez également en mesure de voir les rapports précédents, chaque fois que vous consultez le rapport après avoir lancé un nouveau scan.

Si vous ne voulez pas que d'autres rapports soient créés, il vous suffit d'accéder à "fichier de rapport" dans le menu des options (voir page 25) et décochez la case "Créer un fichier de rapport de boîte.

Les Alertes

avast! est capable d'envoyer un message d'avertissement au sujet d'un incident viral. A partir du menu des options, sélectionnez "Réglages" puis "Alertes". Cette fonction est utile pour les administrateurs de réseau, qui seront informés de la présence de virus sur tout ordinateur se trouvant dans leur réseau, afin qu'ils puissent réagir rapidement.



L'alerte peut être envoyée sous ces formes suivantes:

- **WinPopup.**
  Cliquez sur "Ajouter" et sélectionnez WinPopup. Puis, entrez l'adresse IP ou le nom réseau de l'ordinateur pour envoyer l'avertissement, ou cliquez sur "Parcourir" et sélectionnez l'adresse dans la liste des options disponibles.

- **MAPI.**
  L'alerte sera envoyée par e-mail, en utilisant le protocole MAPI. Entrez l'adresse à laquelle sera envoyé l'e-mail, puis cliquez sur le bouton MAPI au bas de l'écran, entrez le nom de profil MAPI et le mot de passe correspondant.

- **SMTP.**
  L'alerte sera envoyée par e-mail, en utilisant le protocole SMTP. Pour créer une nouvelle alerte, cliquez sur "Ajouter", puis cliquez sur SMTP. Dans la boîte de dialogue qui apparaît, saisissez l'adresse e-mail de la personne à qui sera envoyée l'alerte. Il est également nécessaire de spécifier certains paramètres d'autres - voir la section suivante, "SMTP".

- **Imprimantes.**
  L'alerte sera envoyée à l'imprimante spécifiée. Cliquez sur "Ajouter", puis "imprimante", puis cliquez sur "Parcourir" et sélectionnez l'imprimante à partir de la liste des options disponibles.

  Entrez l'adresse e-mail que le receveur de l'alerte utilise pour se connecter au service Windows Messenger.

Pour créer une nouvelle alerte, cliquez sur "Ajouter" et sélectionnez le type d'alerte nécessaires, puis entrez les informations nécessaires tel que décrit ci-dessus. Une fois l'alerte a été créée, un message sera envoyé au destinataire défini à chaque fois qu'un fichier suspect est détecté.

Pour modifier ou supprimer une alerte qui a été créée, cliquez la-dessus pour la mettre en surbrillance, puis cliquez sur "Modifier" ou "Supprimer".

En cliquant sur "Test" il sera envoye un message de test à l'adresse sélectionnée. En cliquant sur "Tester tous", un message test sera envoyé à tous les receveurs d'alerte se trouvant dans la liste.

SMTP

En cliquant sur SMTP dans la liste à gauche de l’écran, vous pouvez spécifier les paramètres de votre serveur SMTP. avast! utilisera ces paramètres pour envoyer des e-mail, en particulier lors de:

• L’envoi des messages d'avertissement (Alertes) quand un virus a été trouvé.
• L’envoi de fichiers à partir de la zone de quarantaine à ALWIL Software.
• L’envoi des rapports d'erreur d'avast! à ALWIL Software.

Vous devez entrer les informations suivantes:

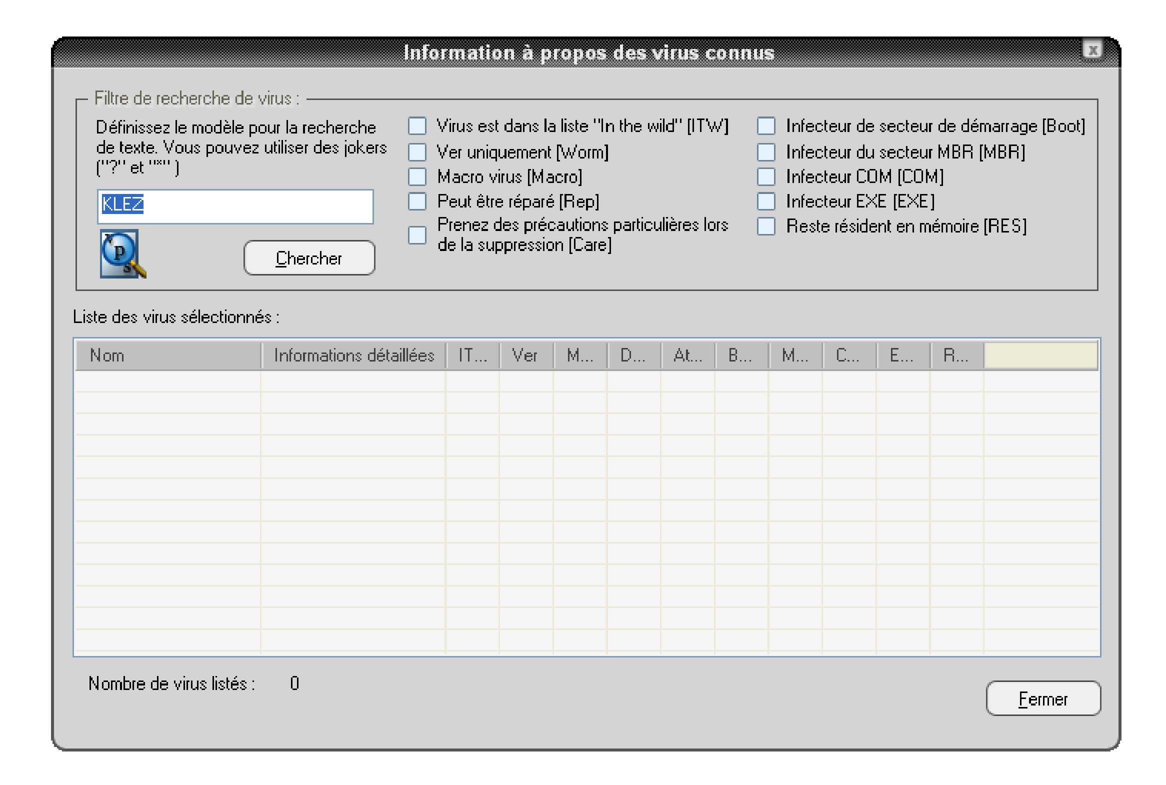
• Adresse du serveur - l'adresse de l'ancien serveur de messagerie (par exemple smtp.server.com ou 192.168.1.25).
• Port - le numéro du port (la valeur par défaut est 25).
• A partir de l'adresse - adresse de l'expéditeur ("De").

Si le serveur SMTP requiert une authentification lorsque vous vous connectez, vous devez également cocher la case et entrez le nom d'utilisateur et mot de passe.

Recherche dans la base de données virale

La base de données virale contient des informations détaillées sur tous les virus connus et elle est utilisée par le programme afin d'identifier d'éventuelles infections.

Pour accéder à la base de données virale, ouvrez le menu des options (voir page 25) et cliquez sur " base de données virale". L'écran suivant s'affichera:



Les virus contenus dans la liste peuvent être recherchés par de nombreux paramètres. Si vous connaissez le nom du virus, il suffit de taper le nom dans la case et cliquez sur le bouton Rechercher. Si vous connaissez seulement une partie du nom, vous pouvez taper "?" à la place d'un caractère inconnu de (lettre ou numéro) ou "*" à la place de plusieurs caractères inconnus.

Exemple: Supposons que vous recherchez le virus "Klez". Son nom réel dans la base de données est Win32: Klez-H [WRM]. Il faut donc taper: * klez *. Tous les virus contenant le mot "klez" seront alors trouvés.

Pour affiner la recherche, vous pouvez également utiliser les cases à cocher à côté de chaque caractéristique de virus. Pour effectuer une recherche sur une caractéristique particulière, cochez la case en cliquant deux fois. Cliquez sur une case à cocher une seule fois, pour que cela se change en couleur grise ce qui signifie qu'il ne doit pas avoir cette fonction. Si une case à gauche n'est pas cochée, mais est de couleur bleue/verte, cela signifie qu'il n'est pas important de savoir si le virus a cette fonction ou non.

Les caractéristiques de virus possibles à chercher:

- ***Virus dans la liste “In the wild” (ITW)***
  Le virus se trouve sur la liste des virus les plus répandus parmi les utilisateurs du monde entier.

- ***Vers uniquement (Worm)***
  Il s'agit d'un type de virus qui n’infecte pas directement les fichiers, mais effectue d'autres actions indésirables tels qu’en se propageant eux-mêmes via e-mail, en volant les mots de passe etc

- ***Macro virus (Macro)***
  Ce type de virus utilise le langage macro en particulier des produits Microsoft (par exemple Word, Excel).

- ***Peut-être réparé (Rep)***
  Fichiers infectés par ces virus et qui peuvent-être réparés et restaurés à leur état d'origine avant l'infection par le programme d’avast!

- ***Prenez des précautions particulières lors de la suppression (Care)***
  Pour ces virus, il est nécessaire de suivre des mesures spéciales lors de leur suppression (sinon, les dommages qui seront faits peuvent-être plus grand que ceux qui auraient été causées par le virus lui-même!).

- ***Infecteur du secteur de démarrage (Boot)***
  Ce type de virus infecte le secteur de démarrage d'un disque dur ou disquette.

- ***Infecteur du secteur MBR (MBR)***
  Ce type de virus infecte le secteur de démarrage principal d'un disque dur.

- ***Infecteur COM (COM)***
  Ce type de virus infecte les fichiers exécutables ayant l’extension ".com".

- ***Infecteur EXE (EXE)***
  Ce type de virus infecte les fichiers exécutables ayant l’extension ".exe".

- ***Reste résident en mémoire (RES)***
  Ces virus restent dans la mémoire RAM de l'ordinateur et infectent les fichiers quand ils sont demarrés.

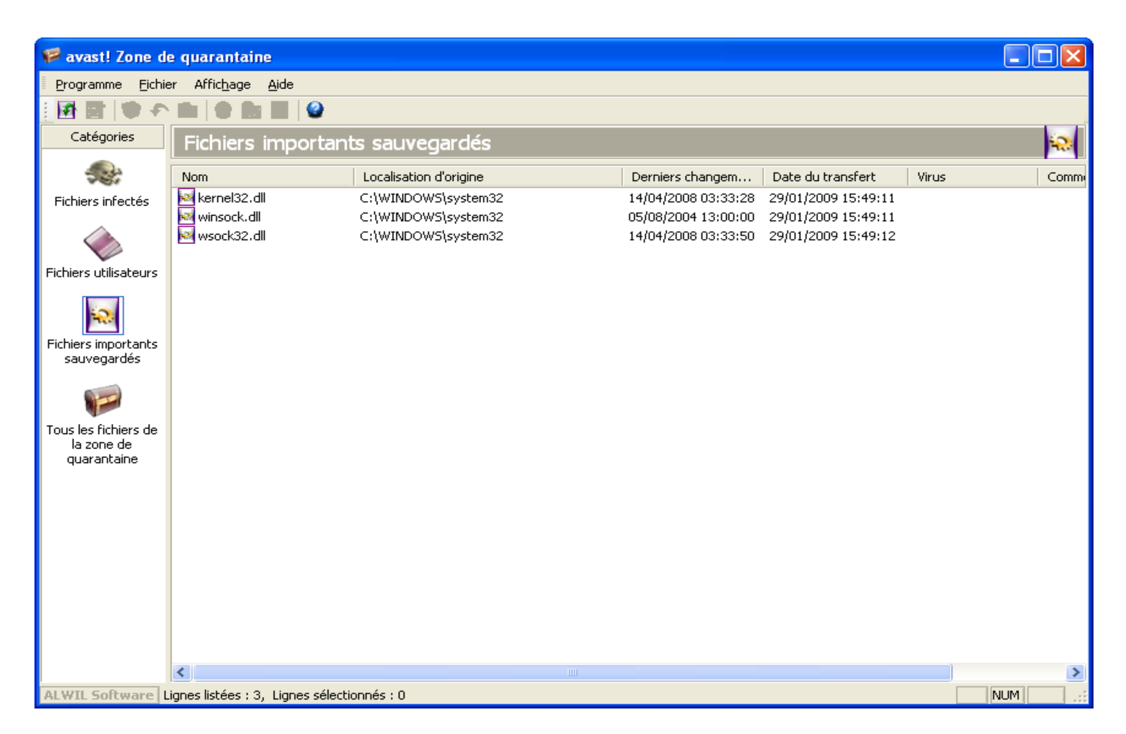
Travailler avec des fichiers se trouvant dans la zone de quarantaine

On peut acceder aux virus de la zone de quarantaine directement depuis le menu des options. En raison de ses propriétés uniques, la zone de quarantaine est effectivement une «quarantaine», qui peut donc être utilisé pour les buts suivants:

- ***Stockage de virus.***
  Si avast! détecte un virus et que vous décidez de ne pas le supprimer, pour une raison quelconque, vous aurez la possibilité de l’envoyer dans la zone de quarantaine. Avec le virus dans la quarantaine, vous pouvez être sûr qu'il ne sera pas exécuté par accident.

- ***Stockage de fichiers suspects.***
  La zone de quarantaine est utile pour stocker tout fichier suspect pour une analyse future.

- ***Sauvegarde des fichiers systèmes.***
  Au cours de l'installation, des copies de certains fichiers système critiques est stockées dans la quarantaine, sous la catégorie "Fichiers importants sauvegardés"(voir ci-dessous). Si les principaux fichiers du système sont infectés par un virus, les copies peuvent être restaurées à partir de la quarantaine vers leur emplacement d'origine.



En faisant un clic droit un fichier, vous aurez les options suivantes. Alternativement, faites un clic gauche sur un fichier pour le mettre en surbrillance, puis cliquer sur l'icône correspondante en haut de l'écran ou cliquez sur "Fichier" et sélectionnez l'option requise *(Note: Si vous **double-cliquez** sur un fichier, vous ne l'exécuterez pas – ses proprietes*

seront affichées à la place. Il s'agit d'une mesure de sécurité pour vous protéger contre une infection accidentelle à partir de la quarantaine):

- ***Actualiser tous fichiers***
  Sélectionnez cette option si vous voulez vous assurer que vous êtes à la recherche à la liste complète des fichiers. Le programme de la liste actualisée automatiquement, mais vous pouvez utiliser cette option si vous ne voulez pas attendre.

- ***Ajouter.***
  Vous pouvez ajouter des fichiers uniquement à la catégorie "fichiers utilisateurs".

- ***Supprimer.***
  Si vous sélectionnez cette option, le fichier sera supprimé de façon irréversible, c'est-à-dire les fichiers ne sont pas tout simplement mis dans la corbeille. Avant de supprimer un fichier, assurez-vous que ce n'est pas un fichier système. La suppression d'un fichier système peut avoir des conséquences très graves.

- ***Restaurer.***
  Le fichier va être restauré à son emplacement d'origine et en même temps retiré de la quarantaine.

- ***Extraire.***
  Le fichier sera copié dans le dossier sélectionné.

- ***Scanner.***
  Le fichier sera analysé.

- ***Propriétés.***
  Les propriétés du fichier sont affichées; il est possible d'ajouter un commentaire au fichier.

- ***Email à ALWIL Software.***
  Le fichier sélectionné sera envoyé (par e-mail) à ALWIL Software. Vous devriez utiliser cette option que dans des cas particuliers - par exemple si vous pensez que le programme a de manière incorrecte identifié un fichier comme un virus. N'oubliez pas d'inclure autant d'informations que possible - par exemple la raison pour laquelle vous envoyez le fichier, la version de votre base de virus, etc. Cela permettra d'améliorer le service que nous vous fournissons

En cliquant sur "Programme" puis sur "Réglages" et enfin sur "Zone de quarantaine", vous pouvez ajuster la taille maximale autorisée pour la quarantaine, et donc la taille maximale de l'espace qu'il prend sur votre ordinateur.Vous pouvez également spécifier la taille maximale de chaque fichier qui doit être envoyé dans la quarantaine.

Visualiseur de journaux

Après un scan, avast! antivirus crée plusieurs fichiers journaux dans lesquels les informations sur les erreurs ou les fichiers suspects sont stockées. Les informations sur l’installation et les mises à jour du programme et de la base de virus peuvent également y être trouvées. Pour consulter ces fichiers logs, il suffit de sélectionner "Visualiseur de journaux" dans le menu des options (voir page 25).

Les informations contenues dans les fichiers logs sont catégorisées comme suit:

Information	Tout juste l’information selon laquelle tout est OK.
Conseil	Information importante, tout est OK. Cela inclut l’information concernant les mises à jour du programme et de la base de données virale.
Avertissement	Une erreur s'est produite ou un virus a été identifié, mais le programme peut fonctionner ou résoudre le problème.
Erreur	Une erreur s'est produite, le programme ne peut fonctionner.
Critique	Une erreur critique du programme, le programme sera fermé.
Alerte	Il ya un risque possible pour l'ensemble de l'ordinateur.
Urgence	Dangereux pour tout l'ordinateur (sécurité, suppression des fichiers système).

En cliquant sur "Fichier" puis sur "Réglages" enfin sur "Journaux", vous pouvez ajuster la taille maximale de chaque fichier dans le journal.

Dans le Visualiseur de journaux, il est possible de rechercher des données spécifiques, de filtrer les données selon des critères précis, ou d'exporter les donnees vers un autre emplacement.

Chercher une donnée

1. Appuyez en meme temps sur les touches “CTRL” et “F”, ou
2. Cliquez sur “Edition” dans le coin supérieur droit de la fenêtre puis sur “Chercher”, ou
3. Cliquez sur la loupe dans le coin supérieur gauche de la fenêtre, ou
4. Faites un clic-droit sur la liste des données et ensuite cliquez sur “chercher” dans le menu affiché.

Une boîte de dialogue apparaîtra où vous pouvez saisir tout ou une partie du nom de la donnée que vous souhaitez rechercher. Si vous connaissez le nom exact, cocher la case

"Mot entier uniquement" assurera que les correspondances exactes sont répertoriées. De même, si vous voulez uniquement rechercher des données en utilisant les majuscules ou minuscules, cochez la case "Respecter la casse". En cliquant sur "Haut" ou "Bas", cela déterminera l'ordre dans lequel les données seront listées (ordre croissant ou décroissant).

Ensuite, cliquez sur "Suivant". La première donnée sera affichée. Toutes les autres données qui correspondent au nom entré peuvent être trouvées en cliquant sur "Rechercher le suivant", jusqu'à ce qu'il n'y ait plus de données trouvables.

Filtrer la liste des données. Il est utilisé pour réduire une longue liste de données afin d'obtenir une petite liste de données qui répondent à certains critères, par exemple un mot clé ou une partie d'un mot.

1. appuyez en même temps sur les touches "CTRL" et "R", ou
2. cliquez sur "Edition" dans le coin supérieur gauche de l'écran, puis sur "Filtrer", ou
3. cliquez sur l'entonnoir jaune dans le coin supérieur gauche de l'écran, ou
4. clic-droit sur la liste des données, puis cliquez sur "Filtrer" dans le menu affiché.

Une boîte de dialogue apparaîtra alors dans laquelle vous pouvez spécifier les critères de filtrage:

Inclure
Entrez un mot clé ou une partie d'un mot qui devrait être inclus dans les données qui seront affichées. Vous pouvez utiliser des métacaractères c'est-à-dire vous pouvez taper * à la place de toutes lettres que vous ne connaissez pas. Plusieurs mots-clés doivent être séparés par un point-virgule (;).

Exclure.
Entrez un mot clé ou une partie d'un mot qui ne doit pas être inclus dans les données qui seront affichés.

Plage de temps
Ici, vous pouvez définir le début et la fin de la période pour laquelle vous souhaitez que les données soient affichées.

Sélectinnez des lignes définies
Si cette option est sélectionnée, les données qui correspondent aux critères définis seront simplement mises en évidence dans la liste.

Afficher uniquement lignes définies (cacher le reste)
Si cette option est sélectionnée, seuls les donnees qui correspondent à la définition des critères seront affichées. Les autres données ne seront pas visibles. Ceci est utile si la liste est très longue.

Trier les données
Un clic sur l'un des en-têtes de colonne permettra de trier les données en ordre croissant ou décroissant en fonction de l'information contenue dans cette colonne. Un clic sur le titre de la colonne fera retourner la liste à l'ordre original.

Exporter les données
Les données Trouvées ou filtrées, ou l'ensemble de la liste de données peuvent être exportés et enregistrés dans un nouveau fichier. Pour exporter des données trouvées ou filtrées, sélectionnez l'option "Exporter les lignes choisies” ou en cliquant sur la flèche verte à gauche dans le coin en haut à gauche de l'écran. Pour exporter la totalité de la liste, choisissez "Exporter la liste actuelle" ou cliquez sur la flèche verte à droite. Dans la nouvelle fenêtre qui s'affiche, choisissez le dossier de destination pour le fichier exporté et tapez le nouveau nom du fichier, puis cliquez sur “Enregistrer”.

Réglages de la Protection Résidente

1. Messagerie instantanée

Programmes

Ici vous pouvez spécifier les programmes de messagerie instantanée pour lesquels les fichiers doivent être scannés. Si vous utilisez Windows 95/98/ME, et que vous souhaitez protéger le programme Trillian, vous devez entrer le chemin d'accès à son fichier de configuration, talk.ini (vous pouvez utiliser le bouton Parcourir pour cela). Certains programmes ne peuvent être protégés que si vous utilisez Windows NT, 2000, XP, 2003, Vista ou 2008.

2. Courier Electronique

Sur les pages "POP", "SMTP", "IMAP" et "NNTP" vous pouvez spécifier si les courriers entrants et/ou sortants et les news seront analysés. Si un virus est détecté, une alerte sera insérée dans le message. Vous pouvez également spécifier que la note soit insérée dans les courriers sains confirmant qu’ils sont exempts de toute infection virale.

Rediriger

Cette page vous permet de régler une analyse transparente des courriels. Tout courier qui passe par les ports spécifiés sera analysé. Cette fonction n’est disponible uniquement que sur les systèmes d’exploitation basés sur la technologie NT (Windows NT/2000/XP/2003/Vista/2008).

- Ports redirigés.

  Les ports par défaut sont les numéros de port standard pour les quatre protocoles d'e-mail: Si vous utilisez un autre port (ou ports), ils doivent être indiquées ici. Plusieurs valeurs doivent être séparées par des virgules.

- Adresses ignorées.

  Ici vous pouvez entrer les adresses des serveurs de messagerie ou des ports spécifiques que vous voulez exclure de l'analyse. Cette fonctionnalité peut-être utile lorsque vous souhaitez qu'avast! analyse uniquement des messages d'un compte particulier (et ignore le reste). Par exemple, si vous entrez smtp.server.com, avast! n'analysera pas les messages sortants (SMTP) pour le compte correspondant.

- Ignorer la communication en local.

  Cette option devrait normalement être cochée. Si elle est décochée, avast! analysera même la communication locale (qui est généralement sans danger), ce qui peut ralentir légèrement votre ordinateur. Note: Ne pas indiquer des numéros de port autres que ceux que vous utilisez pour le trafic e-mail. Sinon, des problèmes inattendus peuvent se produire.

Avancé

- Affiche les infos détaillées sur l'action exécutée.

  Si cette case est cochée, les informations sur les fichiers actuellement en cours d'analyse seront affichées dans le coin inférieur droit de l'écran.

- Mode silencieux.

  Si l'action indiquée sur la page Virus est l'action par défaut c'est-à-dire l'option interactive, et le mode silencieux est sélectionné, les fichiers infectés seront traitées automatiquement, selon les règles suivantes:

  - Si "Avec réponse par défaut Oui (OK)" est sélectionné, aucun fichier infecté joint à un e-mail sera automatiquement supprimé.

  - Si la deuxième option "Avec réponse par défaut Non (annuler)" est sélectionné aucun fichier infecté ne sera automatiquement transféré dans la zone de quarantaine.

  Si l'action indiquée sur la page des Virus est l'action par défaut et cette case est décochée, l'écran normal alerte de virus s'affichera et vous demandera la manière dont vous voulez traiter le fichier infecté.

  Si aucune autre action n'est spécifiée, c'est-à-dire qu'en cochant cette case, toute action autre que l'option par défaut interactive, n'aura aucun effet.

  Notez, toutefois, que si une action autre que l'action par défaut a été spécifiée pour le Bouclier Standard, cela va outrepasser l'action spécifiée pour le service de courrier électronique!

- Délai d'expiration de communication Internet.

  C'est le temps en secondes mis pour attendre une réponse du serveur de messagerie. Vous pouvez en outre préciser que la connexion devrait être fermée si aucune réponse n'est reçue dans ce délai ou si la confirmation devrait être d'abord demandée à vous.

- Affiche l'icône dans la zone de notification lors de l'analyse des mails

  Si cette case est cochée, une petite icône s'affiche dans la barre de notification, dans le coin inférieur droit de votre écran d'ordinateur pour indiquer qu'une analyse est en cours.

Heuristiques

avast! peut non seulement analyser le courrier entrant pour la recherche des virus connus, mais il peut aussi vérifier les messages en utilisant une analyse heuristique et peut identifier un virus qui n'est pas encore présent dans la base de données de virus. Vous pouvez modifier les paramètres de l'analyse heuristique sur cette page.

- Sensibilité - basse.

  - Analyse standard des pièces jointes.
    Les pièces jointes sont analysées en fonction de leurs noms et si le nom d'une pièce jointe contient deux extensions, par exemple "Patch.jpg.exe", elle sera traitée comme potentiellement dangereuse. Avast! vérifie aussi si l'extension de la pièce jointe correspond au type de fichier actuel, par exemple si le fichier "Pamela.jpg" est une image, comme espéré, ou un fichier COM renommé

  - Analyse des séquences d'espaces.
    Certains virus ajoutent un certain nombre d'espaces (ou d'autres non affichables, caractères " blanc") à la fin d'une extension de fichier, suivi d'une seconde, véritable extension qui est dangereuse. En raison de la longueur du nom de fichier, l'utilisateur peut ne pas voir la deuxième extension, cependant l'analyse heuristique peut découvrir cette astuce. La valeur par défaut du nombre espaces consécutifs permis est de cinq. S'il ya plus de cinq, un message d'avertissement sera affiché.

- Sensibilité – Moyenne (En plus de ce qui précède).

  - Analyse standard des pièces jointes.
    Aussi bien que la vérification des pièces jointes, un avertissement sera affiché si l'attachement est un simple exécutable d'extension (EXE, COM, BAT, etc.) Ce ne sont pas tous des fichiers dangereux et ce niveau de

sensibilité va donc générer plus de faux positifs que les alertes de vérification de base des pièces jointes.

- Sensibilité - Haute. (En plus de ce qui précède)

  - Annalyse du code HTML.
    Certains virus peuvent exploiter des bugs se trouvant dans certains programmes de messagerie (en particulier MS Outlook et Outlook Express non sécurisés) qui permettent de lancer le virus simplement en affichant le message dans le volet de prévisualisation. avast! vérifie si le code HTML du message contient une balise permettant une telle astuce. Si c'est le cas, un message d'avertissement est affiché.

  - Messages sortants –Tems d'analyse.
    La plupart des virus se propagent par e-mail et s'envoient eux-mêmes à des adresses stockées dans le carnet d'adresses Windows. Dans un temps très court, les messages sont envoyés à un grand nombre d'adresses, sur le même sujet et/ou avec une pièce jointe. avast! surveille le nombre de messages dans un laps de temps et peut également consulter le sujet et/ou les pièces jointes. Ces paramètres peuvent être réglés sur la page Heuristiques (Avancé).

  - Messages sortants – Envoi en masse.
    Les virus peuvent aussi se propager en s'envoyant eux-mêmes en un seul message à plusieurs destinataires. avast! surveille donc le nombre total de destinataires. Le nombre total admissible des destinataires peut être fixé sur la page Heuristiques(Avancé).

- Sensibilité - Personnalisée

  En cliquant sur "Personnaliser", vous pouvez choisir lequel de ces éléments de l'analyse heuristique vous voulez utiliser.

  Vous pouvez également sélectionner une "vérification de la structure du sujet". Si cette option est sélectionnée, l'entête du sujet du message sera vérifiée pour un grand nombre de caractères absurdes, par exemple si le sujet contient la séquence "<?*&$^*(^%#$%*_()", un avertissement sera affiché.

- URLs autorisées

  En cliquant sur "URLs Autorisées", vous pouvez définir toutes les URLs qui sont considérées comme sûres, qui seront alors ignorées par l'analyse heuristique. Pour ajouter une URL, cliquez sur "Ajouter" puis tapez manuellement le nom de l'URL. Pour supprimer une URL, cliquez sur celle-ci une fois pour mettre en surbrillance, puis cliquez sur "Enlever"

- Mode Silencieux

  Sur cette page, vous pouvez également spécifier quelles mesures doivent être prises si un message infecté est détecté.

Heuristiques - Avancé

Cette page vous permet de modifier les paramètres de l'analyse heuristique pour le courrier sortant. Les paramètres ne sont utilisés que lorsque la sensibilité de "heuristique" est réglée sur "haute" ou "Personnalisé" (et ils peuvent être modifiés seulement avec le réglage sensibilité Personnalisée).

- Temps vérifié.

  avast! comptera les messages sortants au cours de la période donnée. Les réglages par défaut sont de 5 messages en 30 secondes. Cela signifie que si plus de 5 messages sont envoyés en une demi-minute, ayant le même sujet et/ou contenant la même pièce jointe, une alerte sera affichée.

- Nombre d'avertissements.

  C'est le nombre de messages permis sans aucun avertissement, où les messages ont le même sujet et/ou contiennent la même pièce jointe. Lorsque ce nombre est dépassé, un avertissement est affiché.

- Vérifier le sujet.

  Si cela est défini, les messages en masse seront identifiés en fonction du sujet du message.

- Vérifier les pièces jointes.

  Si cela est défini, les messages en masse seront identifiés en fonction de la pièce jointe.

- Nombre absolu.

  C'est le nombre total maximum de destinataires, c'est-à-dire les adresses dans les champs À, Carbon Copy (CC) et Blind Carbon Copy (BCC), fixé à 10 par défaut, qui, s'il est dépassé, se traduira par l'affichage d'un avertissement.

3. Bouclier réseau

Le Bouclier Réseau protège votre ordinateur contre les attaques des vers de l'Internet. Il fonctionne de façon similaire à un pare-feu, bien qu'il ne soit pas un substitut pour un.

Réglages

- Afficher les messages d'avertissement

  Si cette case est cochée, un message apparaîtra dans le coin inférieur droit de l'écran à chaque fois qu'une attaque des vers de l'internet est détectée.

- Autoriser l'envoi des informations anonymes de stastisques à propos des URLs bloquées.

  Si cette case est cochée, toutes les informations à propos des URLs bloquées seront envoyées de facon anonyme.

- Historisation des événements

  Si cette case est cochée, l'historique des attaques de ver sera enregistré et affiché sur la page "Dernières attaques". Pour voir cette page, il est nécessaire d'accéder directement aux réglages de la protection résidente c'est-à-dire par un clic droit sur la boule bleue "a" dans la barre des tâches, il ne peut pas être vu par l'accès aux réglages de la protection résidente via la tâche de la protection résidente dans l'interface Utilisateur avancée.

Dernières attaques

Sur cette page, les 10 dernières attaques de ver du réseau seront affichées, si la case "Historisation des événements" a été cochée sur la page précédente. Ceci contient la date et l'heure de l'attaque, le type d'attaque, l'adresse IP et le port d'où elle provient

4. Outlook/Exchange

Scanner

Ici vous pouvez spécifier quel type de messages qui devrait être scanné et si le corps des messages ainsi que les pièces jointes devraient être aussi scannés.

Courrier entrant

Ici vous pouvez spécifier ce qu'il faut faire si un message entrant infecté est détecté, par exemple, il peut être delivré, rejeté (supprimé), ou redirigé vers un autre dossier de courrier. Vous pouvez également préciser si une note doit être insérée dans les

messages infectés et/ou sains, et le format de la note c'est-à-dire TXT ou HTML. Les fichiers joints infectés ou contenus dans un message sont traités selon les paramètres des pages "Stockage de virus" et "Avancé".

Courrier sortant

Ici, vous pouvez préciser si une note doit être insérée dans les messages sains, ainsi que le format de la note, comme ci-dessus. Les messages infectés ne seront pas envoyés du tout. Vous pouvez également préciser que les pièces jointes devraient être scannées au moment où elles sont attachées, plutôt que lorsqu'elles sont envoyées.

Signatures

En utilisant des signatures, il est possible de réduire fortement le nombre de messages qui doivent être scannés. Les signatures sont de petits "timbres" qui sont attachés à des messages sains pour confirmer qu'ils sont exempts de virus. Chaque signature contient la date et l'heure de l'analyse.
Les signatures du service MS Outlook/Exchange sont entièrement compatibles avec celles d'avast! Exchange Server Edition. Par conséquent, les messages testés par le service d'Exchange Server ne seront pas testés de nouveau par le service de MS Outlook/Exchange, ce qui resulte en un temps de transfert plus rapide.

- **Insérer des signatures dans les messages sains**.

  Cette case devrait être cochée si vous voulez des signatures soient ajoutées aux messages sains.

- **Toujours faire confiance aux messages signés**.

  Si cette case est cochée, les messages signés correctement seront toujours dignes de confiance et ne seront pas analysés, quel que soit l'âge de la signature (à moins que la case "Ignorer toujours les signatures plus anciennes que la base de virus courante" soit cochée).

- **Faire confiance aux signatures uniquement jusqu'à**.

  Ici, vous pouvez définir l'âge maximum des signatures pour la confiance. La valeur définie ici peut être masquée par l'option "Ignorer toujours les signatures plus anciennes que la base de virus courrante" - voir ci-dessous.

- **Ignorer toutes les signatures (pas de confiance)**.

  Si cette case est cochée, tous les messages seront analysés, sans tenir compte de la validité de leur signature.

- **Ignorer toujours les signatures plus anciennes que la base de virus courante**.

Si cette case est cochée, les messages qui ont une signature valable seront analysés, si la signature est plus âgée de la base de virus. Cela pourrait être utile, comme un message peut contenir un virus qui a été ajouté à la base de virus après la première analyse. Si le message était de confiance, il ne sera pas analysé et le virus ne serait pas détecté.

Stockage de Virus

Sur cet écran, vous pouvez spécifier que la copie d'une pièce jointe infectée sera enregistrée dans un dossier spécifique sur le disque dur de l'ordinateur. Vous pouvez utiliser le bouton Parcourir pour localiser et sélectionner le dossier. Si vous cochez la case "écraser les fichiers existants", un fichier avec le même nom sera remplacé par le nouveau fichier.

Avancé

- Monde silencieux

  Si l'action indiquée sur la page Virus est l'action par défaut, c'est-à-dire l'option interactive, en cochant cette case, cela va résulter au transfert automatique de tout fichier infecté vers la zone de quaranataine.

  Si l'action indiquée sur la page Virus est l'action par défaut et que cette case est décochée, l'écran standard de l'alerte de virus s'affiche demandant de quelle façon vous voulez traiter le fichier infecté.

  Si aucune autre action n'est spécifiée, c'est-à-dire toute action autre que l'option interactive, en activant cette case il n'y aura aucun effet.

- Affichée infos détaillées sur l'action en cours

  Si cette case est cochée, les informations sur les fichiers actuellement en cours d'analyse seront affichées dans le coin inférieur droit de l'écran.

- Afficher l'icône dans la zone de notification lors de l'analyse des mails

  Si cette case est cochée, une petite icône s'affiche dans la barre des taches, dans le coin inférieur droit de votre écran d'ordinateur pour indiquer qu'une analyse est en cours.

- Safficher l'écran splash lorsque le service se charge

Enfin, si vous entrez votre profil MAPI et le mot de passe, ceux-ci seront utilisées pour afficher la structure de votre dossier de courrier lorsque vous cliquez sur le bouton Parcourir sur la page du courrier entrant.

Heuristiques

Les réglages sur cette pages sont les mêmes que pour le service de courrier électronique

Heuristiques - Avancé

Les réglages sur cette pages sont les mêmes que pour le service de courrier électronique, mais avec deux réglages additionnels:

- Nombre relatif (carnet d’adresse)

  C'est le nombre autorisé de destinataires d'un message unique, exprimé en pourcentage du nombre total d'adresses e-mail dans le carnet d'adresses. Si ce pourcentage est dépassé, un message d'avertissement sera affiché.

- Nombre minimum

- C'est le nombre minimum de destinataires actuels, correspondant au nombre relatif, au-dessous duquel l’avertissement ne sera pas affiché. En d'autres termes, si le nombre relatif est dépassé, l'avertissement ne sera pas affiché si le nombre actuel de destinataires est inférieur au nombre minimum. Exemple: Nombre relatif = 20%, Nombre minimum = 10. Si le nombre d'adresses est de 40 et qu’un message est envoyé à 9 destinataires, le nombre relatif sera dépassé mais l’avertissement ne sera pas affiché parce que le nombre actuel est inférieur à celui du minimum.

5. Bouclier Peer2Peer

Programmes

Sur cette page vous pouvez spécifier les programmes pour lesquels les fichiers reçus devraient être scannés. Certains programmes ne peuvent être protégés uniquement que dans Windows NT, 2000, XP, 2003, Vista ou 2008.

6. Le Bouclier Standard

Scanner (Basic)
Sur cette page, vous pouvez définir ce que doit être scanné par ce module. Il est recommandé que toutes les cases sur cette page soient cochées, ce qui permettra la détection de la plupart des types de virus.

Scanner (Avancé)

Sur cette page, vous pouvez spécifier d'autres fichiers à scanner en fonction de leur extension, soit quand ils sont ouverts, ou quand ils sont créés ou modifiés.

- Analyser les fichiers à l’ouverture.

  Les extensions des autres fichiers à scanner doivent être séparées par une virgule. Vous pouvez utiliser le caractère "?" (Par exemple, si vous voulez que tous les fichiers ouverts .htm et .html soient analysés, entrez "htm", "html" ou utiliser le joker - "ht?" dans ce dernier cas, toutefois, tous les fichiers avec des extensions à partir de "ht", comme"htt", seront analysés).

  - Toujours analyser les fichiers de script WSH.

    Cette option assure que tous les fichiers scripts (Windows Scripting Host) seront analysés.

  - Ne pas analyser les librairies système.

    Les librairies système de confiance ne seront pas analysées à l'ouverture, seule une vérification rapide sera effectuée afin de valider l'authenticité. Cette option peut accélérer un peu le démarrage du système.

- Analyser fichiers créés/modifiés.

  Si cette case est cochée, les fichiers seront analysés au moment où ils seront créés ou modifiés. Vous pouvez également préciser si cela doit être appliqué à:

  - Tous les fichiers, ou

  - Uniquement les fchiers avec les extensions sélectionnées

Si la case "Jeu d’extensions par défaut (recommandé)" est cochée, seuls les fichiers avec les extensions qui sont généralement considérées comme "dangereuses" seront analysés - cliquez sur "Afficher" pour voir la liste par défaut des extensions. Vous pouvez également spécifier des extensions à analyser.

Bloqueur

Sur cette page, vous pouvez spécifier que certaines opérations sont bloquées pour les fichiers avec certaines extensions. Ceci peut être appliqué au " Jeu d’extensions par défaut " - cliquez sur "Afficher" pour voir la liste des extensions par défaut, mais vous pouvez également spécifier des extensions pour les opérations qui doivent être bloquées.

Vous pouvez ensuite spécifier les opérations qui doivent être bloquées pour les types de fichiers specifies. Par exemple : Ouverture du fichier pour ecriture,

Renommer le fichier, supprimer le fichier, ou Formater.

Enfin, vous pouvez spécifier ce qui doit être fait si une opération est celle qui doit être bloquée, mais avast! n'est pas en mesure d'obtenir la confirmation c'est-à-dire si l'opération devrait être autorisée ou refusée.

Avancé

- Affiche infos détaillées sur l’action en cours

  Si cette case est cochée, l’information sur les fichiers en cours d’analyse sera affichée dans le coin inférieur droit de votre écran.

- Mode Silencieux

  Si l'action indiquée sur la page Virus est l'action par défaut c'est-à-dire l'option interactive, et le mode silencieux est sélectionné, les fichiers infectés seront traitées automatiquement, selon les règles suivantes:

  - Si “Avec réponse générale OUI (OK)” est sélectionné, aucune action ne sera lancée vis-à-vis du fichier infecté

  - Si la seconde option “Avec une réponse générale Non (Annuler)” est selectionnée, tout fichier infecté sera automatiquement transféré dans la zone de quarantaine.

  Si l'action indiquée sur la page Virus est l'action par défaut et que cette case est n'est pas cochée, l'écran normal alerte de virus s'affichera et demandera de quelle façon vous voulez traiter le fichier infecté.

  Si aucune autre action n'est spécifiée, c'est-à-dire toute action autre que l'option par défaut interactive, en cochant cette case, cela n'aura aucun effet.

Enfin, vous pouvez spécifier des endroits spécifiques qui ne devraient pas être analysés par ce module. Notez que les emplacements qui ont été exclus de l'analyse de tous les modules ne sont pas affichés dans cette liste.

7. Le Bouclier Web

Le Bouclier Web agit comme un serveur proxy local. Sur les sytèmes d'exploitation basés sur la technologie NT (Windows NT/2000/XP/2003/Vista/2008) la protection est totalement transparente, et il n'est généralement pas nécessaire d'ajuster les paramètres standards. Si vous utilisez Windows 95/98/ME, cependant, il est nécessaire de modifier les paramètres dans Options Internet - en particulier, l'adresse et le port du proxy local comme suit:

Si vous utilisez un réseau local (LAN):	Si vous utilisez une connexion dial-up (modem):
Démarrez Internet Explorer.	Démarrez Internet Explorer.
Sélectionnez Outils puis Options Internet ... à partir du menu principal.	Sélectionnez Outils puis Options Internet ... à partir du menu principal.
Passez à la page Connexions	Passez à la page Connexions
Cliquez sur paramètres du réseau local	Sélectionnez votre connexion dial-up à partir de liste et cliquez sur "Paramètres".
Cochez l'option "Utiliser un serveur proxy pour votre reséau local…"	Cochez l'option "Utiliser un serveur proxy pour cette connexion".
Ecrivez "localhost" dans le champ Adresse (alternativement, vous pouvez entrer l'adresse IP 127.0.0.1, qui est la même que localhost). Entrer 12080 dans le champ du Port.	Ecrivez "localhost" dans le champ Adresse (alternativement, vous pouvez entrer l'adresse IP 127.0.0.1, qui est la même que localhost). Entrer 12080 dans le champ du Port.
Confirmez en cliquant sur OK.	Confirmez en cliquant sur OK.

Note: Si vous utilisez des connexions multiples, il est nécessaire de définir l'adresse et le port du proxy local pour chaque connexion séparément.

Basique

- Activer l'analyse du contenu Web

  En décochant cette case, vous pouvez désactiver la fonction d'analyse web sans affecter le blocage d'URL, qui restera actif.

- Utiliser l'analyse intelligente des streams

  Si cette case est cochée, les fichiers qui sont téléchargés sont scannés presque en temps réel. Les éléments de données sont analysés dès leur arrivée - et les

prochaines parties sont téléchargées que lorsque les parties précédentes sont vérifiées et sont exempts de virus. Si cette fonctionnalité est désactivée, les fichiers seront téléchargés dans un dossier temporaire d'abord, puis scannées.

Les autres options sur cette page ne sont pas disponibles sur Windows 95, 98, et Millennium:

- Ports (s) HTTP Redirigé(s).

  Ce paramètre est important si vous utilisez un type de serveur proxy pour accéder à Internet et que vous souhaitez analyser la communication entre le serveur et votre ordinateur. Si vous vous connectez à un serveur proxy en utilisant par exemple port 3128, entrez ce numéro dans la case. Sinon, avast! attendra que la communication se fasse via le port 80 (par défaut) et tout le reste sera ignoré. Note: Ne pas entrer tout autre port que HTTP (tels que les ports pour ICQ, DC + +, etc.) Plusieurs numéros de port doivent être séparés par des virgules.

- Adresses Ignorées.

  Ici, vous devez saisir des noms du serveur ou les adresses IP qui ne seront pas redirigés vers le Bouclier Web. Plusieurs adresses doivent être séparées par des virgules.

- Ignorer les communications en local.

  Si cette case est cochée, toutes les communications locales - c'est-à-dire la communication entre les programmes exécutés sur votre ordinateur, seront ignorées.

Analyse Web

Sur cette page, vous pouvez spécifier quels fichiers devraient être scannés lorsqu'ils sont téléchargés de l'Internet. Vous pouvez spécifier que tous les fichiers devraient être scannés ou seulement ceux possedant des extensions particulières. Si vous choisissez ce dernier, vous devez saisir les extensions des fichiers à scanner, séparées par des virgules. Vous pouvez également entrer les types MIME des fichiers qui devraient être scannés. Dans les deux cas, des caractères peuvent être utilisés.

Exceptions

Ici vous pouvez spécifier les objets qui ne seront pas analysés par le Bouclier Web. Cela peut être utile lorsque vous téléchargez un grand nombre de fichiers à partir d'un seul emplacement (de confiance!)

- URLs à exclure

  Utilisez le bouton Ajouter pour entrer les adresses URL qui devront être ignorées. Si vous voulez bloquer une page seulement, il est nécessaire d'entrer le chemin d'accès complet, par exemple si vous ajoutez http://www.yahoo.com/index.html, seulement la page index.html sera exclua de l'analyse. Si vous entrez http://www.yahoo.com/*, cependant, aucune page à partir de http://www.yahoo.com ne sera scannée. De même, si vous voulez un type de fichier à exclure de l'analyse, par exemple, fichiers avec l'extension ".txt", il suffit d'entrer *.txt.

- Types MIME à exclure

  Ici vous pouvez spécifier les types MIME / sous-types a exclure de l'analyse.

Blocage des URL

Le Bouclier Web peut également être utilisé pour bloquer l'accès à certaines pages Web. Il est désactivé par défaut, cependant, il peut être utilisé pour empêcher l'accès à des pages web "impropres" (contenant de la pornographie, des logiciels illégaux, etc.) Si une telle page bloquée est demandée à partir du navigateur Web, un message s'affiche indiquant que l'accès à la page a été bloqué par avast! antivirus.

La case "Activer le blocage des URL" doit d'abord être cochée et vous pouvez alors entrer les adresses à bloquer en cliquant sur le bouton "Ajouter" et ensuite entrer les URL. Les caracteres (c'est-à-dire? Et*) peuvent être utilisés, par exemple, si vous entrez http://www.penthouse.com/*, aucune page à partir de http://www.penthouse.com sera affichée

Les adresses URL Entrées seront complétées selon les règles suivantes:

Si l'adresse ne commence pas par http:// ou jokers * ou?, Avast! ajoute le préfixe http:// au début de l'adresse et ajoute un astérisque à la fin. Donc, si vous entrez www.yahoo.com, il sera modifié à http://www.yahoo.com *.

Avancé

- Affiche infos détaillées sur l'action en cours

  Si cette case est cochée, l'information sur les fichiers en cours d'analyse sera affichée dans le coin inférieur droit de votre écran.

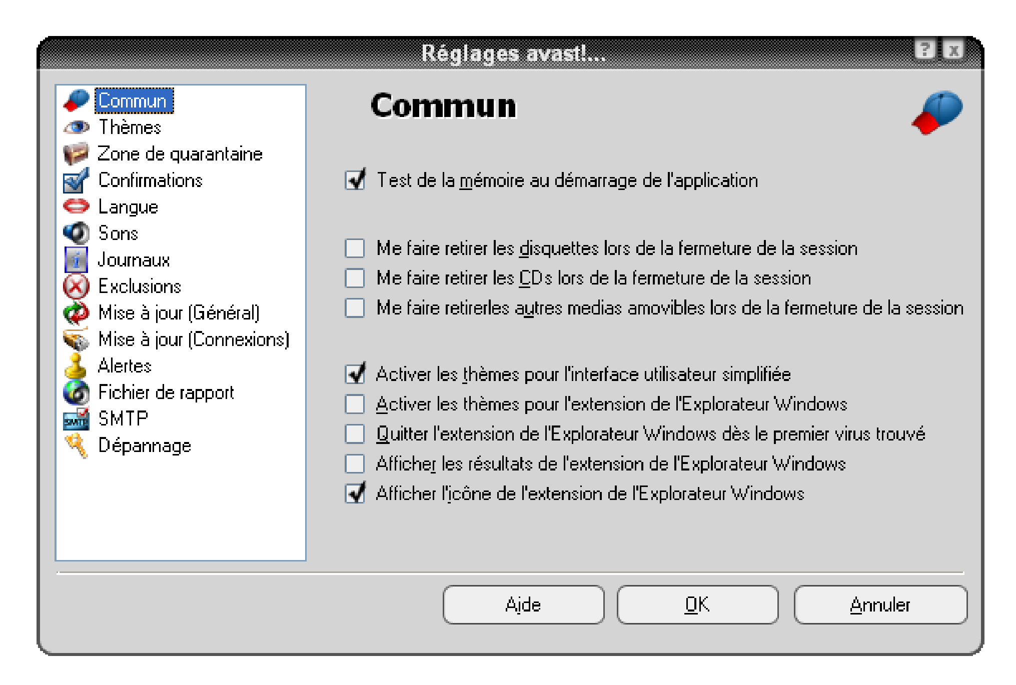
- Mode Silencieux

  Si cette case est cochée, la connexion sera terminée si un virus est détecté

Autres réglages d'avast!

Beaucoup d'autres parties du programme d'avast! sont susceptibles d'être modifiés en fonction de vos propres besoins ou préférences. Certains d'entre elles ont déjà été décrites dans les sections précédentes.

Si vous utilisez l'interface simple et que vous ouvrez le menu des options (voir page 25) et cliquez sur "Réglages", l'écran suivant s'affiche. Si vous utilisez l'interface utilisateur avancée, il vous suffit de cliquer sur "Réglages" et il y aura aussi une option supplémentaire - "l'Interface Utilisateur Avancée". Les différents paramètres peuvent être modifiés en cliquant sur la rubrique correspondante sur le côté gauche de l'écran:



Common

Dans cet écran, vous pourrez spécifier quels sont les contrôles qui sont pris en compte lors du démarrage ou l'arret de votre ordinateur. Ici, vous pouvez aussi changer l'apparence du programme en cochant ou décochant la case "Activer les thèmes ...".

L'extension de l'Explorateur

Les quatre dernières cases à l'écran correspondent à "l'extension de l'Explorateur". Il s'agit de la possibilité de scanner tout fichier en cliquant avec le bouton droit sur ce dernier et de sélectionner l'option "Analyse<nom_fichier>". Si la dernière case est cochée, cette option aura l'icône de la boule bleue "a" à côté.

Thèmes

En cliquant sur "Thèmes" vous pouvez spécifier si l’icône d’avast! – la boule bleue "a" - est indiquée dans le coin en bas à droite de l'écran, et aussi si elle est animée (en rotation), pendant que l’analyse est en cours.

Vous pouvez ajouter un effet translucide à l'apparition du lecteur avast! Ces changements prendront effet après redémarrage de votre ordinateur.

Confirmations

Cet écran vous permet de déterminer si oui ou non il vous sera demandé une confirmation lorsque vous sélectionnez certaines actions, et aussi si vous recevez des messages de confirmation après que certaines actions ont été menées.

La confirmation des requêtes sont une caractéristique de sécurité d'avast! antivirus pour vous permettre d'annuler une action qui est sélectionnée par erreur.

Si vous ne souhaitez pas recevoir de message de confirmation ou de requête, il suffit de le désélectionner en décochant la case appropriée. Toutefois, si une requête de confirmation n'est pas cochée, l'action sera réalisée dès que l'action correspondante est sélectionnée sans la possibilité de l'annuler.

Les confirmations/requêtes suivantes sont activées par défaut, mais peuvent être désactivées en décochant les cases relatives:

- ***Demander avant de fermer l’interface Utilisateur Simplifiée quand un scan est en cours***
  Si le programme est fermé pendant que le scan est en cours, le scan sera automatiquement terminé à ce point

- ***Demander s’il faut perdurer le changement d’état du service résident***
  Ce message apparaît si vous décidez de “Mettre fin à” tout module séparé de protection résidente - voir page 22. Si vous répondez "Oui", le module sera désactivé jusqu'à ce que vous le réactiviez manuellement. Si vous répondez "Non", il sera réactivé la prochaine fois que vous redémarrez votre ordinateur.

- ***Demander avant d’arrêter la protection résidente***
  Ce message apparaît si vous décidez de “Mettre fin à” la protection résidence (ou à l'accès) dans son ensemble - voir page 20. Si vous répondez "Oui", la protection résidente est désactivée, mais elle sera automatiquement réactivée la prochaine fois que vous redémarrez votre ordinateur.

- ***Demander avant la suppression des fichiers de Quarantaine***
  Si cette case est cochée, le programme demandera toujours une confirmation avant de supprimer tout fichier. Il s'agit d'éviter la suppression accidentelle de tous les fichiers

- ***Message lorsque les résultats ont été traités avec succès***
  Cela confirme que toute action que vous avez sélectionné à l'égard de tous les fichiers signalés par le programme, par exemple supprimer, déplacer le fichier vers la zone de quarantaine, etc a été accomplie

- ***Message lorsqu’une erreur s’est produite lors du traitement des résultats***
  Cela vous informe que l’action que vous aviez sélectionnée en fonction d’un fichier signalé par le programme ne peut être effectuée.

- ***Message lorsq’un fichier VPS trop vieux est utilisé***
  Cela est pour vous avertir que la base de virus n'est pas à jour. Pour vous assurer que votre système est entièrement protégé, la base de virus doit être régulièrement mise à jour – voir page 37

- ***Avertissement concernant la version BETA du programme***
  Ce message est pour vous avertir que la version du programme que vous utilisez est toujours dans sa phase de test.

- ***Afficher un message lorsque le rapport d’erreur a été envoyé avec succès***

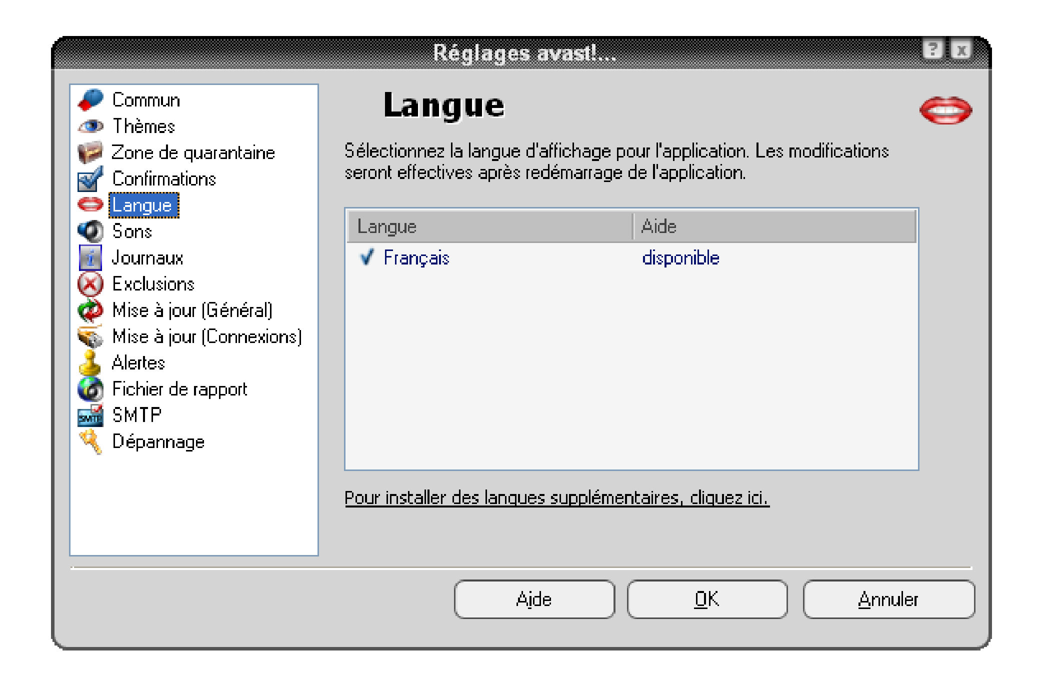
- ***Afficher la fenêtre d’état dans la zone de quarantaine même si l’action s’est bien déroulée OK***
  Si cette case est cochée, vous recevrez un message pour confirmer que l'action que vous avez sélectionné a été traitée avec succès.

- ***Message lorsque les résultats Ok sont activés pendant la configuration de la tâche.***
  Lorsque cette case est cochée, vous verrez un avertissement si vous spécifiez que les "fichiers OK" doivent être inclus dans l'analyse des résultats. Remarque, cela ne s'applique qu'à la création de tâches dans l'interface utilisateur avancée.

- ***Suppression des fichiers avec une extension dangereuse***
  Ceci est un avertissement pour assurer que vous ne supprimerez pas un fichier spécifié dont le type est celui qui contient normalement des données importantes.

Changement de la langue du programme

Si vous voulez changer la langue de programme, cliquez sur "Langue" et l'écran suivant s'affichera:



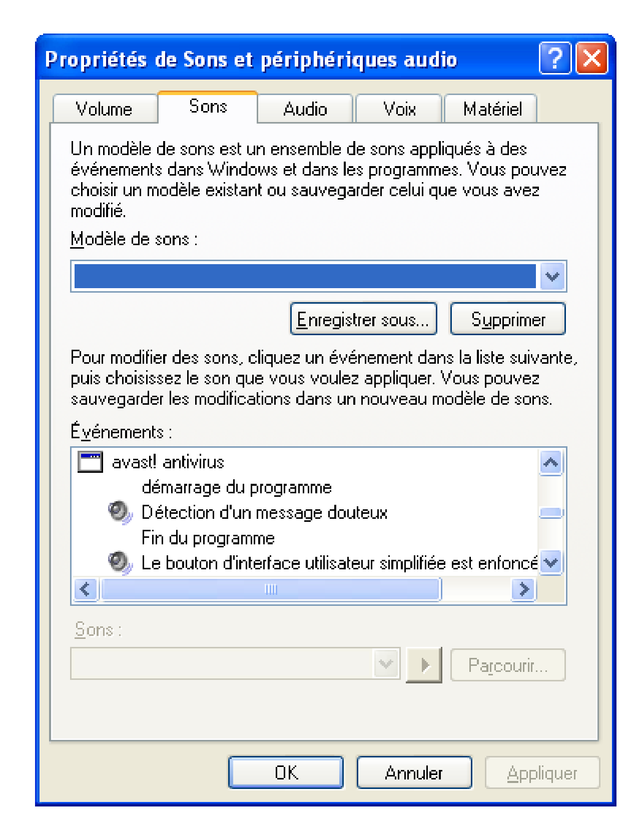
Si la langue est alors affichée comme "disponible" dans la case de droite, cliquez dessus pour la sélectionner, puis cliquez sur "OK". Et la langue sera modifiée la prochaine fois que vous redémarrez votre ordinateur.

Si la langue n'est pas affichée comme "disponible", cliquez sur "Pour installer des langues supplémentaires, cliquez ici" au bas de la case, puis cochez la case relative à la langue dont vous avez besoin. Cliquez sur "Suivant" et tous les autres fichiers du programme seront installés. Une fois terminé, cliquez sur "Terminer"
Vous pouvez désormais sélectionner la langue souhaitée comme décrit ci-dessus.

Sons

Dans cet écran, vous pouvez ajuster les paramètres audio du programme ou vous pouvez désactiver complètement les effets sonores.

Si vous cliquez sur le bouton "Paramètres" de nouveau, cela vous affichera un écran où vous pouvez ajuster les paramètres de son de tous les programmes Windows. Dans la moitié inférieure de l'écran, il ya une case intitulée "Evénements" - voir ci-dessous.



Si vous cliquez sur la flèche bleue vers le bas sur le côté droit, à mi-chemin dans la liste, vous trouverez les événements de sons d’avast! antivirus qui peuvent être affectés. Si vous voulez affecter un nouveau son à un événement, cliquez sur l'événement et ensuite sur "Parcourir". Dans la liste des options disponibles, sélectionner le son que vous souhaitez et cliquez sur "OK".

Vous pourrez alors revenir à la case ci-dessus où vous devez cliquer sur "Appliquer" puis sur "OK" de nouveau.

Cela vous ramènera à l’écran principal des "Sons" où vous devriez cliquer de nouveau sur "OK" pour finir.

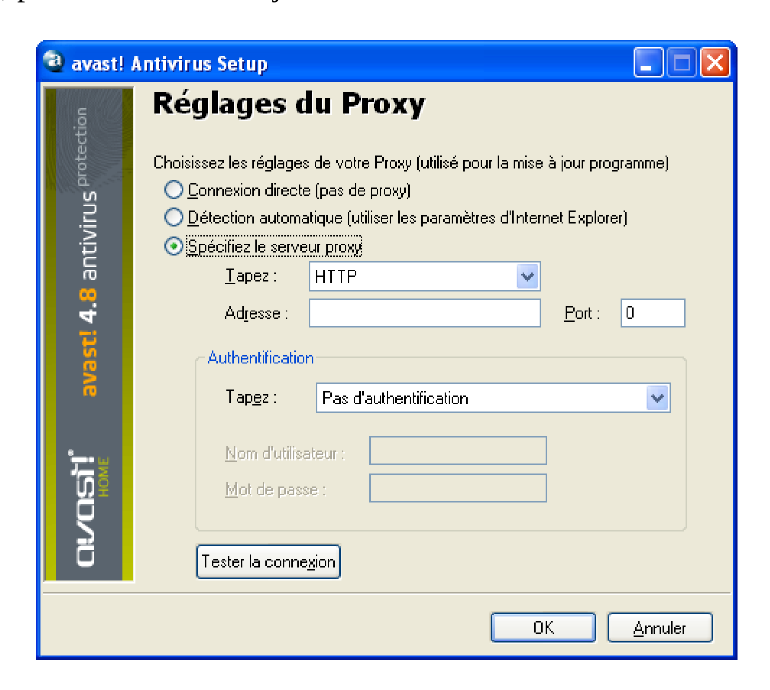
Mise à jour (Connexions)

Sur cet écran, vous pouvez spécifier le type de connexion internet en sélectionnant l'option appropriée.

- Je me connecte à Internet à l'aide d'un modem téléphonique, ou
- Mon ordinateur est connecté de manière permamente à Internet

Cela permettra d'optimiser la façon dont avast! vérifie la présence de nouvelles mises à jour et permettra au processus de mise à jour automatique d'être plus fiable.

Une fois que vous avez spécifié le type de connexion, cliquez sur le bouton "Proxy". Cela ouvrira une nouvelle fenêtre où vous pouvez entrer les paramètres du serveur proxy. Les paramètres du serveur proxy sont importants lorsqu'avast! a besoin d'accéder à l'Internet, par exemple, pendant les mises à jour.



Si vous vous connectez directement à Internet (c'est-à-dire une connexion sans proxy), qui s'applique généralement aux utilisateurs des connexions téléphoniques, sélectionnez l'option "Connexion directe (pas de proxy)"

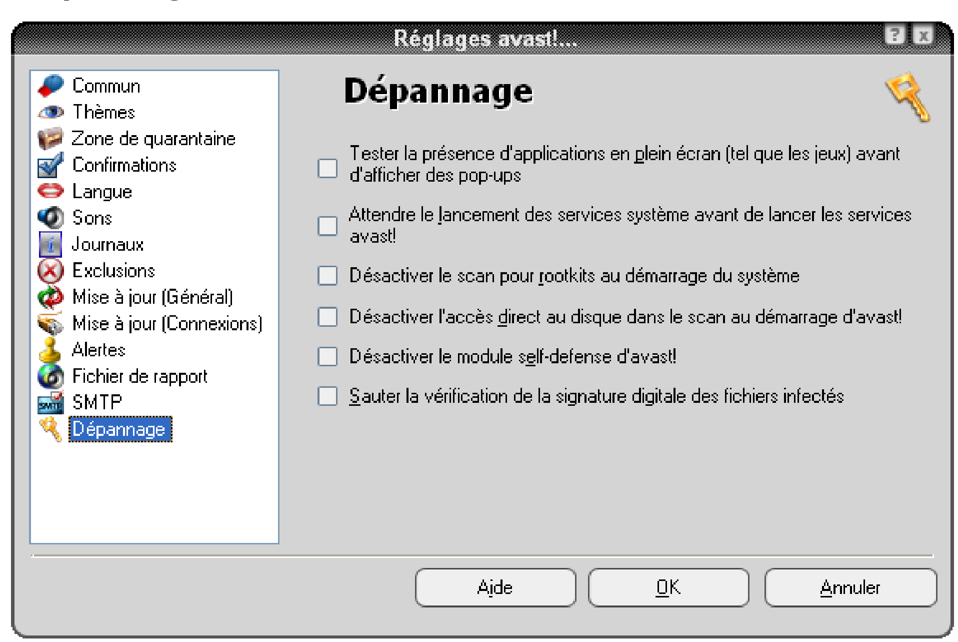
Si vous ne savez pas si vous utilisez un serveur proxy, ou celui que vous utilisez, sélectionnez "detection automatique (utilisez les paramètres d'Internet Explorer), ou demandez à votre fournisseur de service Internet ou à votre administrateur réseau.

Si vous connaissez l'adresse et le port de votre serveur proxy, sélectionnez "Spécifier le serveur proxy" et entrez les informations requises comme suit:

- **Tapez**. Soit HTTP ou SOCKS4
- **Adresse**. Entrez l'adresse de votre serveur proxy.
- **Port**. Entrez le port que votre serveur proxy utilise.
- **Authentication tapez**. Spécifiez ici si l'accès à l'Internet via votre serveur proxy requiert une authentification de l'utilisateur, et si nécessaire, le type d'authentification.
- **Nom d'utilisateur et mot de passe**. Ceux-ci devraient être entrés si l'authentification est requise.

Finallement, cliquez sur "Tester la connexion" pour tester si la connexion Internet (basée sur les réglages ci-dessus) fonctionne correctement.

Dépannage



Le changement des paramètres sur cette page peut aider à résoudre certains problèmes spécifiques. Toutefois, ces paramètres ne devraient pas être modifiés sans bonne raison. En cas de doute, s'il vous plaît contactez premièrement avast!.

Tester la présence d'applications en plein écran (tel que les jeux) avant d'afficher des pop-ups.

Selon votre configuration d'avast!, de divers messages peuvent etre affichés lorsque votre ordinateur est en cours d'exécution (par exemple, lorsque la base de données de virus a été mise à jour, quand un e-mail est analyse pour la detection de virus, etc.) Normalement, les messages sont affichés chaque fois que l'événement correspondant se produit. Ceci peut cependant interrompre les applications en plein écran (par exemple les jeux)- Windows passe du mode plein écran en mode normal lorsque la fenêtre de message apparaît. Si vous cochez cette option, avast! essaie de détecter si une application en plein écran est en cours d'exécution avant d'afficher un message, si une application en plein écran est trouvé, avast! n'affiche pas le message.

Attendre la lancement des services système avant de lancer les services d’avast !.
Le service d'avast! antivirus est habituellement démarré très tôt pendant le processus de démarrage. Parfois, cela peut causer des problèmes lors du démarrage du système d'autres services - ce qui pourrait se manifester par exemple comme le gel temporaire (pour quelques secondes ou minutes) de ce système, peu après qu'il est commencé. Cette option permet de retarder le démarrage du service d'avast! antivirus jusqu'à ce que le système habituel des services soit entièrement chargés.

Désactiver le scan pour rootkits au démarrage du système.
avast! analyse pour rechercher les rootkits à chaque fois que vous démarrez le système d'exploitation. Cochez cette case si vous souhaitez désactiver ce type d'analyse.

Désactiver l’accès direct au disque dans le scan au démarrage d’avast !.
Au cours de l'analyse en temps de démarrage, avast! utilise une méthode d'accès de disque qui permet à l'antivirus de détecter les virus qui cachent leurs fichiers. Ici, vous pouvez désactiver cette fonctionnalité - avast! utilisera la méthode d'accès de disque habituelle.

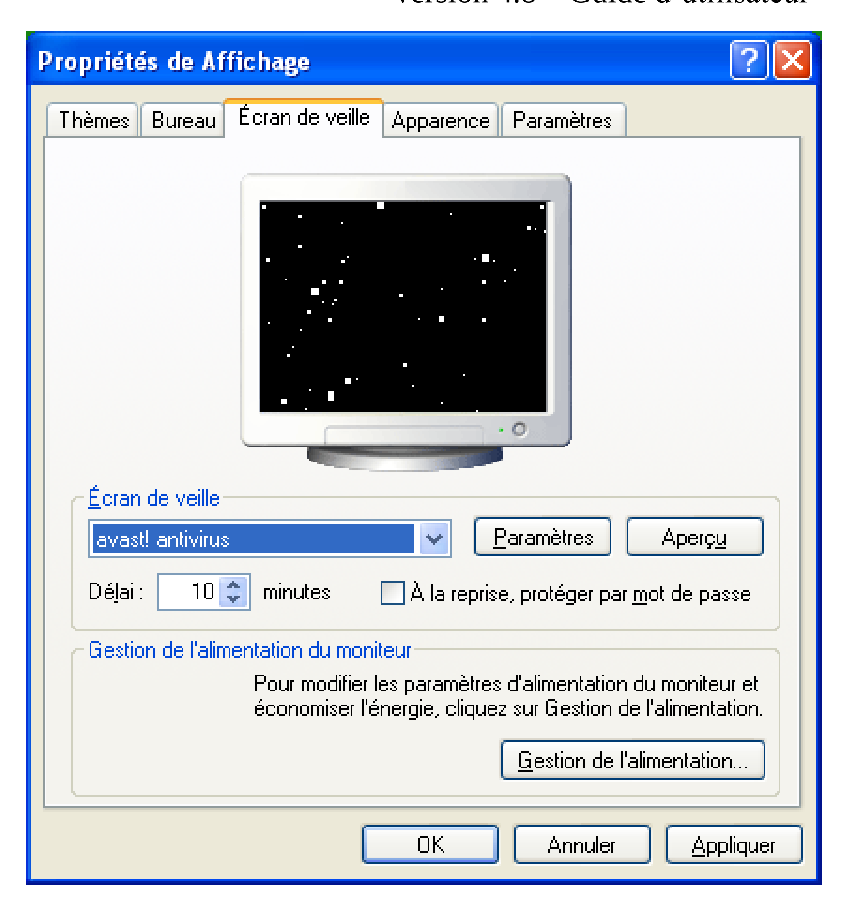
Désactiver le module self-defense d’avast !.
Certains virus sont capables de désactiver les logiciels antivirus en mettant fin à ses processus, en supprimant ou en modifiant ses fichiers critiques. avast! contient des fonctionnalités de self-défense qui empêchent ces attaques en bloquant les opérations dangereuses. Afin de désactiver ce module d'auto-défense, cochez cette case.

Sauter la vérification de la signature digitale des fichiers infectés.
Pour éviter les fausses alertes positive, avast! contrôle les signatures numériques des fichiers infectés. Si un fichier est détecté comme infecté, mais il contient également une signature numérique valide d'une autorité de confiance (par exemple, Microsoft), cela est probablement un faux positif - et avast! ignore cette (fausse) détection. Cochez cette case pour désactiver la vérification supplémentaire - avast! signalera toutes les infections qu'il trouve.

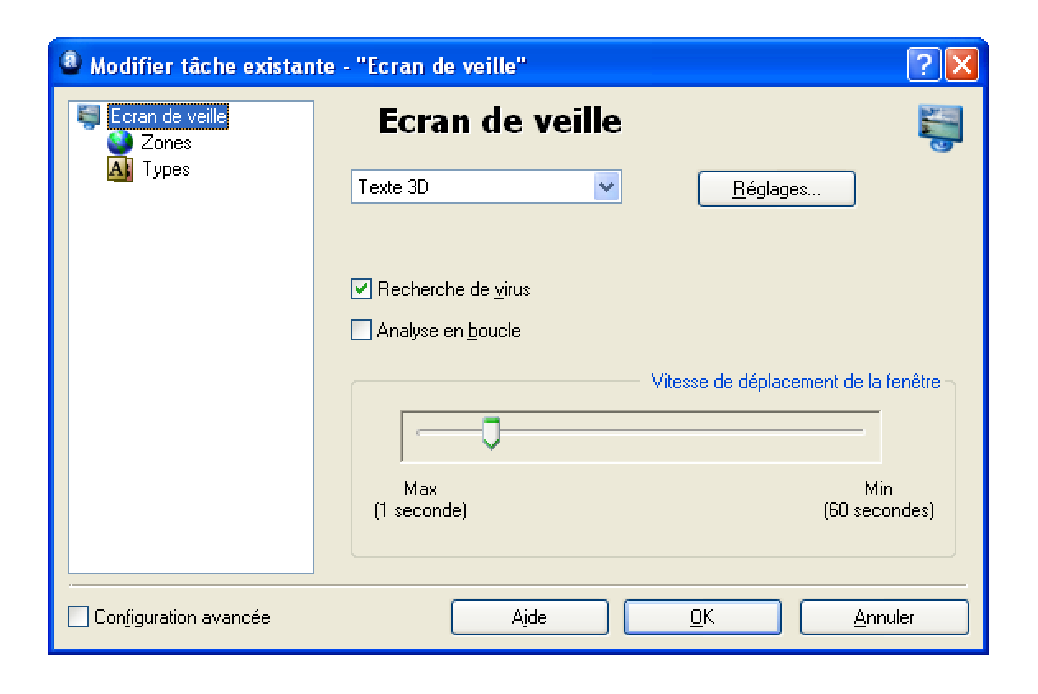
Comment activer l’écran de veille d’avast! antivirus

Avast! antivirus est capable de scanner votre ordinateur en vue de prevenir une eventuelle infection virale pendant que l'ordinateur n'est pas en service et que l'économiseur d'écran est activé. Pendant ce temps, une petite boîte est affichée dans l'écran de veille et affiche les informations sur la progression de l’analyse.

Pour activer l’écran de veille d'avast! antivirus, faites un clic-droit à n’importe quel endroit vide de votre bureau. Ensuite dans le menu contextuel qui apparaîtra cliquez sur "Propriétés". Dans la boîte qui s’affichera, cliquez sur l’onglet "Ecran de veille", puis sur la première flèche bleue pour voir les options disponibles. Sélectionnez "avast! antivirus". Dans la case ci-dessous, vous pouvez également modifier le nombre de minutes après lesquelles l'économiseur d'écran devrait être activé, en utilisant les flèches bleues haut/bas, et si nécessaire entrez votre mot de passe pour continuer.



En cliquant sur "Paramètres" dans cet écran, vous pouvez sélectionner l'économiseur d'écran normal au sein duquel apparaîtra la boîte d'avast! affichant le message d'information sur le statut de l'analyse - voir la page suivante.



Si vous voulez que votre ordinateur soit analyse pour la recherche de virus chaque fois que l'économiseur d'écran est activé, cochez la case "Recherche de virus". Si cette case n'est pas cochée, l'écran de veille fonctionnera seulement comme un économiseur d'écran normal.

En cochant la case "Analyse en boucle", cela veillera à ce que le scan soit lancé de nouveau une fois que toutes les zones définies auront été analysées.

La modification de la vitesse de déplacement de la fenêtre aura une incidence sur la fréquence de positionnement de la boite de progression d’analyse sur l'écran.

En cliquant sur "Paramètres" de nouveau vous permettra d'ajuster les paramètres de l'économiseur d'écran normal.

En cliquant sur "Zones", vous pouvez spécifier les zones de votre ordinateur qui doivent être analysées. Les zones à scanner automatiquement y compris "Tous les disques durs". Si vous ne voulez pas que tous les disques durs soient scannés, supprimez cette option en cliquant sur elle-ci et puis en cliquant sur "Supprimer". Vous pouvez ensuite spécifier les zones à scanner en cliquant sur «Parcourir» et en sélectionnant la ou les zones en cochant les cases appropriées. En cliquant sur "Ajouter" vous pouvez choisir parmi un certain nombre de zones prédéfinies.

Une fois que vous avez sélectionné la ou les zones à scanner, cliquez sur "Types" pour spécifier les types fichiers que vous desirez analyser. Les fichiers peuvent être reconnus en tant que suspects en fonction de leur contenu, ce qui est plus complet et donc plus lents, ou en fonction de leur extension de nom.

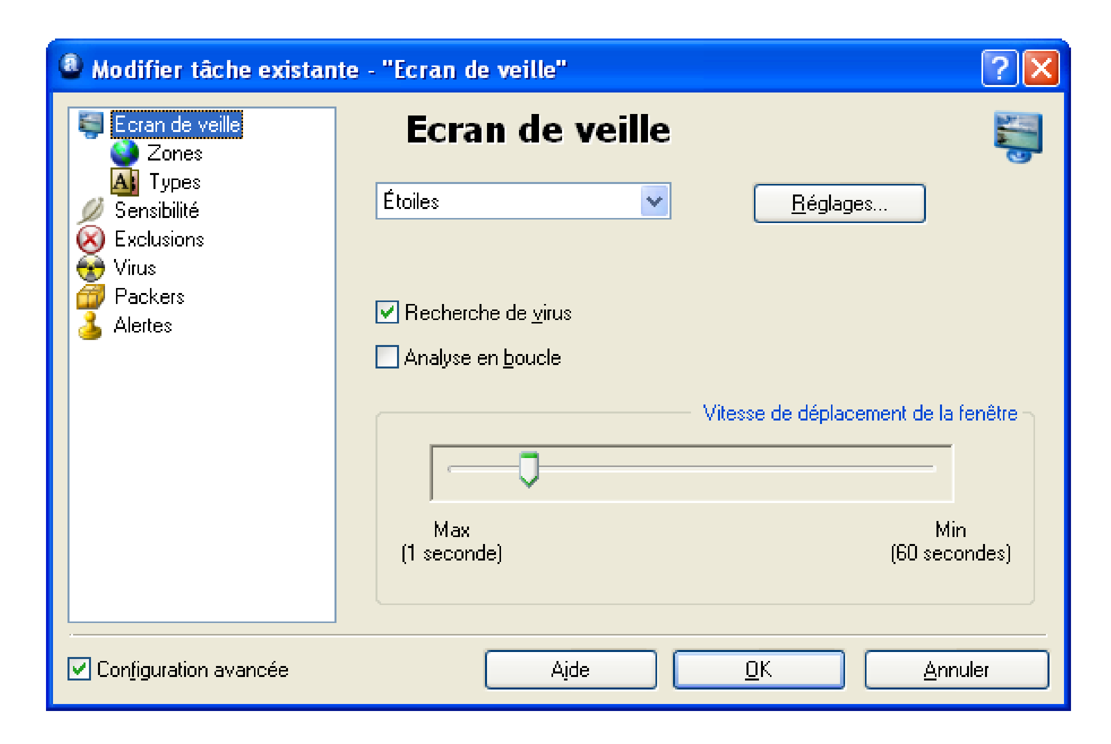
Si vous sélectionnez une analyse en fonction du contenu, vous pouvez spécifier que tous les fichiers devront être analysés en cochant la case "Scanner tous les fichiers". Si vous cochez cette case, cela signifie que même les fichiers qui n'ont pas l'habitude de contenir des virus, tels que les fichiers image, seront également analysés. Si vous laissez cette case décochée, ces fichiers ne seront pas scannés et seront signalés comme "fichiers ignorés".

Si vous sélectionnez une analyse en fonction de l’extension, vous devriez spécifier les extensions qui devraient être reconnus comme suspecte.

Pour analyser les fichiers sur la base d'une ou plusieurs extensions, cliquez sur "Parcourir" et une liste d'extensions de fichiers sera affichée. Si vous pouvez trouver l'extension que vous souhaitez ajouter, cliquez sur celle-ci puis cliquez sur "OK" pour l'ajouter à la liste. Si l'extension que vous souhaitez ajouter n'est pas dans la liste, vous pouvez l'ajouter manuellement. Cliquez sur "Ajouter" puis tapez l'extension du fichier que vous souhaitez ajouter. Pour ajouter une autre extension, cliquez sur "Ajouter" de nouveau. Si vous souhaitez supprimer un fichier d'extension de la liste, il suffit de cliquer dessus pour le mettre en surbrillance, puis cliquez sur "Supprimer".

Si la case "Scan des extensions par défaut" est cochée, cela signifie que toutes les extensions "dangereuses" et connues seront automatiquement scannées. Tous les fichiers avec des extensions autres que celles spécifiées seront ignorés pendant l’analyse.

Si vous cochez la case "Configuration avancée", un certain nombre d’option sera affiche – voir ci-dessous.



- ***Sensibilité***

En cochant la case "Tester les fichiers en entier (très lent pour les gros fichiers), cela permettra aux fichiers d’être testés entièrement plutôt que les parties les plus fréquemment touchées par des virus. La plupart des virus se trouvent soit au début d'un fichier, ou à la fin. Cochez cette case pour aboutir à une analyse plus approfondie, mais aussi ralentir la le scan.

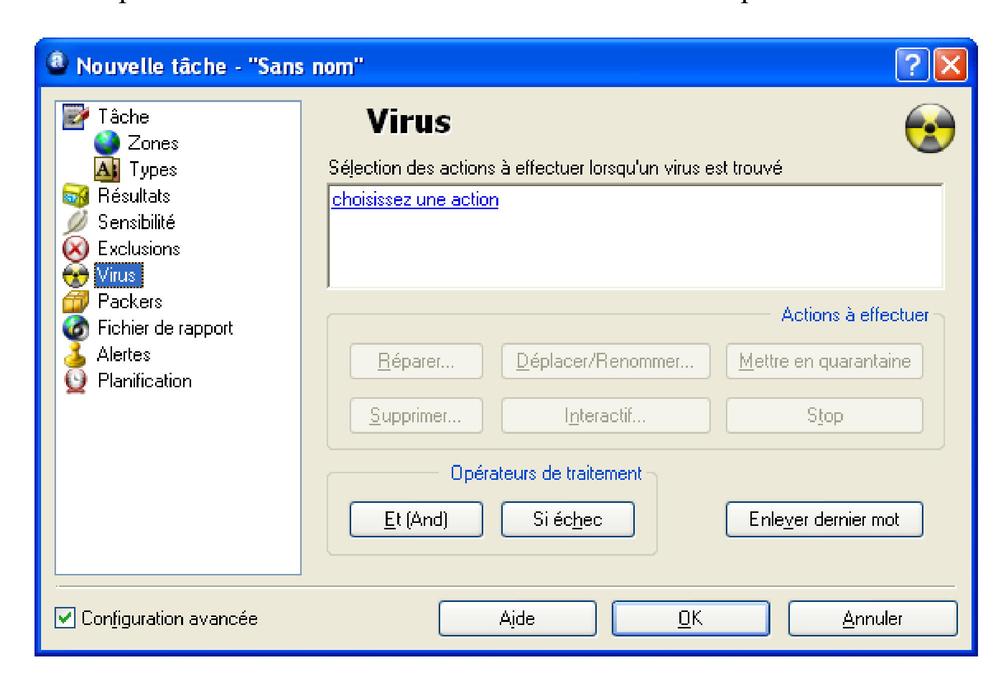
En cochant la case "Ignorer le ciblage des virus", cela signifie que les fichiers seront analyses en fonction de tous les virus dans la base de virus. Si ce n'est pas coché, les fichiers seront testés uniquement en fonction des virus qui affectent ce type de fichier. Par exemple, le programme ne sera ne recherchera pas les virus qui infectent les fichiers en ".exe" dans les fichiers d'extension ".com".

- ***Exclusions***

Ici, il est possible d'exclure de l'analyse certains fichiers ou dossiers. Cela fonctionne exactement de la même manière que décrite à la page 40, à l'exception que les exclusions définies ici ne s'appliquent qu'à la tâche spécifique. Les fichiers ou dossiers qui sont exclus dans le menu "Réglages" seront automatiquement exclus de toutes les analyses. Les fichiers qui sont exclus seront rapportés dans les résultats de la session en tant que "fichiers ignorés"

- ***Virus***

En cliquant sur "Virus" vous aurez la fenêtre suivante qui s'affichera:



Sur cet écran, vous pouvez spécifier quelles mesures doivent être prises quand un virus est détecté. La valeur par défaut est "choisissez une action". Il s'agit dune option "Interactive".

Si cela n'est que l'action sélectionnée, cela signifie que chaque fois qu'un fichier suspect est détecté, il vous sera présenté une liste d'options parmi lesquelles vous devrez faire votre sélection. Cela signifie que vous pouvez spécifier individuellement les mesures à prendre pour chaque fichier suspect.

En cliquant sur "Choisissez une action" il vous sera affiché les options qui seront présentées à chaque fois un fichier suspect est détecté, c'est-à-dire : Supprimer, Réparer, Mettre en quarantaine, Déplacer/Renommer, ou Stop. Seules les options qui sont cochées seront présentées comme les options disponibles. Si aucune option n'est cochée, elle ne sera pas présentée comme une option disponible quand un fichier suspect sera détecté.
Ces options sont décrites à la page 32 dans la section "Que faire lorsqu'un virus est détecté".

La sélection de cette action entrainera la suspension de l'analyse si un virus est détecté jusqu'à ce que vous indiquiez les mesures à prendre. Par conséquent, il est recommandé de choisir une ou plusieurs des autres actions, telles que déplacer le fichier vers la quarantaine, si vous programmez la tâche à s'exécuter à un moment où vous êtes absent.

Pour sélectionner une autre action, cliquez sur le bouton "Enlever dernier mot". L'action par défaut sera alors supprimée et les six actions possibles seront maintenant mises en évidence au centre de l'écran. En cliquant sur l'un d'entre eux, l'action va insérer dans la case ci-

dessus. Cette action sera ensuite appliquée à tous les fichiers suspects qui sont détectés. Pour l'enlever, il suffit de cliquer de nouveau sur "Enlever dernier mot".

Les quatre premières actions sont décrites en détail à la page 32. En cliquant sur "Interactif", cela va ré-insérer "choisissez une action". En cliquant simplement sur Stop, cela arrêtera l'analyse dès qu'un fichier suspect est détecté.

Il est possible de spécifier plus d'une action en utilisant le bouton "et(And)". Par exemple, vous pouvez spécifier que tous les fichiers infectés seront réparés et déplacés vers un autre emplacement en cliquant sur "Réparer" puis "et" puis "Déplacer/Renommer".

Vous pouvez également préciser toutes les autres actions alternatives qui devraient être prises si la première action sélectionnée échoue. Par exemple, vous pouvez choisir "réparer" comme la meilleure action, mais en cliquant sur "Si échec" et "Metrre en quarantaine", vous pouvez faire en sorte que tous les fichiers qui ne peuvent pas être réparés soient placés vers la quarantaine - voir page 48.

Note - si vous sélectionnez "Supprimer", vous serez plus loin à mesure de préciser si le fichier doit être supprimé de façon permanente (par défaut), ou tout simplement doit être mis dans la corbeille. Si vous sélectionnez l'option "Supprimer le fichier de façon permanente", vous serez également en mesure de préciser si le fichier devrait être supprimé la prochaine fois que l'ordinateur est redémarré, s'il ne peut pas être supprimé maintenant, en cochant la case "Si nécessaire, supprimer le fichier au prochain démarrage du système".

- ***Packers***

Sur cette page, vous pouvez spécifier quels sont les fichiers archives seront testés au cours de la tâche. Le réglage par défaut est uniquement auto-extractible exécutable. Vous pouvez spécifier que les archives additionnelles doivent être traitées, même si cela aura pour effet de ralentir l'analyse. Cochez la case "Tous les formats" si vous voulez que tous les fichiers archives qui peuvent être analysés soient scannés.

- ***Alertes***

Les alertes peuvent être soit des alertes générales, qui seront envoyées chaque fois qu'un virus est détecté, ou elles peuvent être générées que si un virus est détecté par la tâche à laquelle elles sont liées.

Les alertes qui peuvent être ajoutées à la tâche sont présentées dans la boîte "Alertes disponibles".

Les alertes générales sont créées en cliquant sur "Réglages" et "Alertes" tel que décrit à la page 44, toutefois, les alertes qui ont été créées de cette manière ne peuvent être liées à une tâche.

Si l'alerte que vous souhaitez ajouter est montrée ici, cliquez dessus pour la mettre en surbrillance, ensuite cliquez sur le button "→". Cela déplacera l'alerte dans la boite "Alertes utilisées", ce qui signifie qu'elle est désormais liée à la tâche.

Si l'alerte que vous souhaitez ajouter n'est pas affichée, cliquez sur "Nouveau" pour créer une nouvelle alerte.

Vous pouvez assigner un nom à l'alerte, par exemple, un nom qui le relie à la tâche et vous pouvez ajouter d'autres informations dans la boîte de "Commentaire". L'alerte est alors créée de la même manière que décrit à la page 44

Une fois que vous avez créé la nouvelle alerte, cliquez sur OK et elle sera automatiquement placée dans la boîte "Alertes utilisées".

Pour supprimer un message d'alerte de la boite "Alertes utilisées", cliquez sur elle pour la mettre en surbrillance, puis cliquez sur bouton "←", qui se déplacera de nouveau vers la boîte "Alertes disponibles".

Pour modifier ou supprimer une alerte, sélectionnez-la et cliquez sur "Modifier" ou "Supprimer".

Si vous avez besoin pour créer une alerte SMTP, n'oubliez pas d'indiquer les détails du serveur SMTP une fois que vous avez terminé de créer votre tâche en cliquant sur "Réglages" et "SMTP".

Notez que les alertes liées à des tâches, ne seront envoyées que si un virus est détecté par la tâche spécifique. Elles ne seront pas envoyées si le virus est détecté par une autre tâche. Si vous souhaitez qu'une alerte soit envoyée à chaque fois qu'un virus est détecté par une tâche, vous devez créer une alerte générale telle que décrite à la page 44.

Comment mettre à niveau vers l'Edition Professionnelle

Mise à niveau de l'Edition familiale vers l'edition Professionnelle est très simple.

Vous n'avez pas besoin de désinstaller la version actuelle du programme et aucun téléchargement n'est nécessaire. Vous avez juste besoin d'acheter de l'Edition Professionnelle, pour obtenir la clé de licence et l'insérer dans votre programme actuel. Les autres composants seront alors téléchargés automatiquement et votre programme sera mis à niveau immédiatement vers l'Edition Professionnelle.
Une clé de licence peut être achetée pour 12, 24, ou 36 mois - il vous suffit d'accéder à www.avast.com et de cliquer sur "Acheter".

Comment désinstaller avast! antivirus

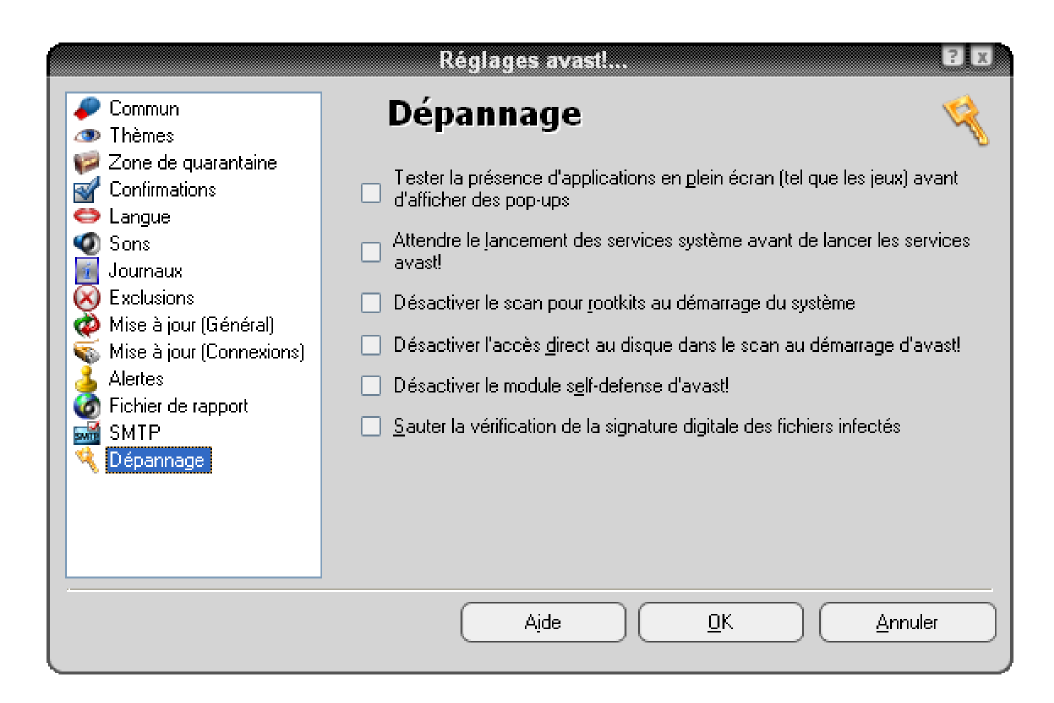
Certains virus sont conçus pour éteindre le logiciel d'antivirus d'un ordinateur. Par conséquent, avast! antivirus est désormais protégé par un puissant module d'auto-défense (SD) qui l'empêche d'être modifié ou supprimé par ces virus. Toutefois, une conséquence est que les autres programmes valides peuvent trouver difficile de modifier ou de supprimer avast! antivirus par rapport aux versions précédentes. Afin de bien désinstaller le programme d'avast! antivirus, il est essentiel de suivre la procédure requise.

Avant d'essayer de désinstaller avast! antivirus, il est recommandé de fermer toutes les autres applications que vous pourriez avoir sur votre ordinateur. Pour désinstaller avast! antivirus, la procédure recommandée est la suivante.

1. Désactivez le module Self Defense

- Cliquez avec le bouton droit sur la boule bleue "a" dans le coin inférieur droit de votre écran d'ordinateur et dans le menu des options, sélectionnez "Réglages du programme…".

- Cliquez sur "Dépannage" dans la colonne de gauche et vous aurez l'écran suivant



- Maintenant, cochez la case "Désactiver le module self-defense d'avast !" et cliquez sur "OK"

- Le module self-defense est maintenant désactivé.

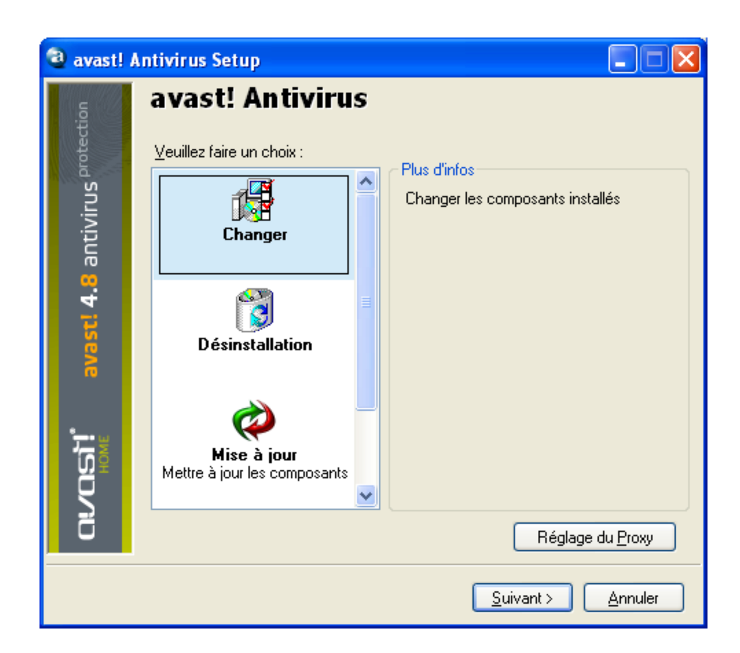
2. Désinstaller le programme

- Cliquez sur "Démarrer" dans le coin inférieur gauche de l'écran de l'ordinateur et ouvrez le panneau de configuration de votre ordinateur. Si vous ne pouvez pas le voir dans le menu Démarrer, cliquez sur Paramètres et elle devrait être affichée comme l'une des options.

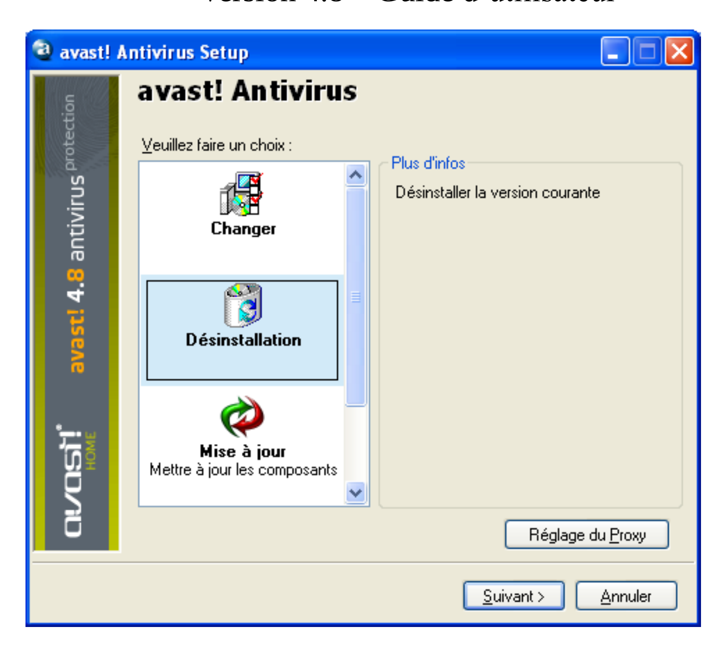
- Dans le Panneau de configuration, cliquez sur "Ajouter ou supprimer des programmes".

- Une liste de tous les programmes installés s'affichera.

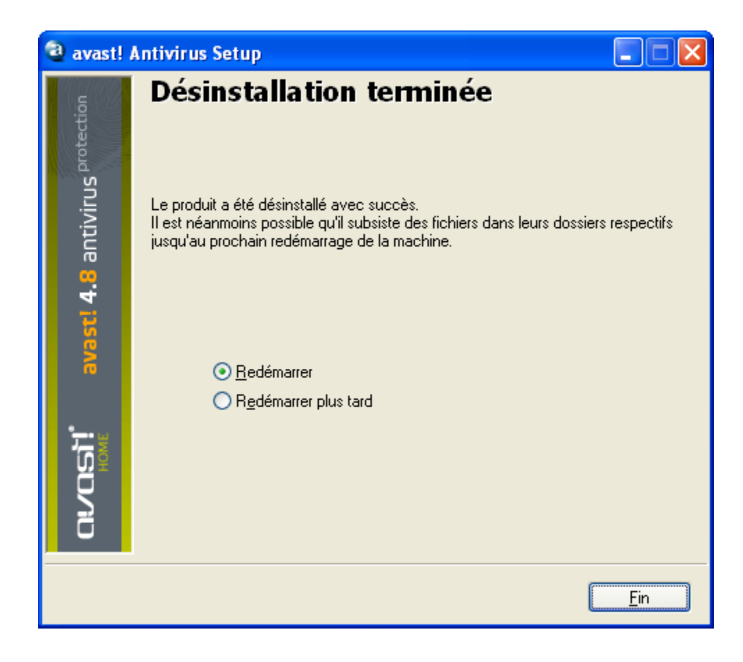
- Sélectionnez "avast! antivirus" en cliquant dessus puis cliquez sur "Modifier/Supprimer"
- L'écran suivant sera affichée:



Cliquez sur "Désinstallation" pour le mettre en evidence et ensuite sur "Suivant"



Le programme sera maintenant désinstatllé, selon ce qui est mentionné sur l'ecran suivant:



Pour compléter le processus de désinstallation, il est nécessaire de redémarrer l'ordinateur. Avec "Redémarrer" sélectionné, cliquez sur "Terminer" et votre ordinateur sera automatiquement redémarré.